Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Industrial
Escuela Profesional de Ingeniería Industrial

Desarrollo de un Sistema de Gestión de Continuidad de Negocio en una entidad financiera, basado en la ISO 22301

TESIS

Para optar el Título Profesional de Ingeniero Industrial

AUTOR

Anthony Joel RÁZURI ESPINOZA

ASESOR

Willy Hugo CALSINA MIRAMIRA

Lima, Perú

2019

Referencia bibliográfica

Rázuri, A. (2019). *Desarrollo de un Sistema de Gestión de Continuidad de Negocio en una entidad financiera, basado en la ISO 22301*. Tesis para optar el título profesional de Ingeniero Industrial. Escuela Profesional de Ingeniería Industrial, Facultad de Ingeniería Industrial, Universidad Nacional Mayor de San Marcos, Lima, Perú.

Metadatos

Código ORCID del autor:	NO APLICA
Código ORCID del asesor:	https://orcid.org/0000-0001-6203-8344
Grupo de investigación:	NO APLICA
Institución financiada parcial o total:	NO APLICA
Ubicación geográfica de la investigación:	Av. República Argentina 5306, Callao
Año o rango de años de la investigación:	2016 – 2018
DNI:	47275843

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMERICA)
FACULTAD DE INGENIERÍA INDUSTRIAL

ACTA N°024-VDAP-FII-2019

SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO INDUSTRIAL

El Jurado designado por la Facultad de Ingeniería Industrial, reunido en acto público en el Auditorio de la Facultad de Ingeniería Industrial, el día **jueves 11 de julio de 2019,** a las 10:00 horas, dio inicio a la sustentación de la tesis:

"DESARROLLO DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO EN UNA ENTIDAD FINANCIERA, BASADO EN LA ISO 22301"

Que presenta el Bachiller:

RÁZURI ESPINOZA, ANTHONY JOEL

Para optar el Título Profesional de Ingeniero Industrial en la Modalidad: **Ordinaria.**

Luego de la exposición, absueltas las preguntas del Jurado y siendo las 11:10 horas se procedió a la evaluación secreta, habiendo sido APROBADO con la calificación promedio de CATORCE, lo cual se comunicó públicamente.

Ciudad Universitaria, 11 de julio del 2019

MG. SALAS BACALLA, JULIO ALEJANDRO
Presidente

MG. RUIZ LIZAMA, EDGAR CRUZ
Miembro

MG. MAVILA HINOJOZA, DANIEL HUMBERTO
Miembro

MG. CALSINA MIRAMIRA, WILLY HUGO
Asesor

Dedicatoria

La presente tesis es dedicada con todo el amor a mis padres y hermana, quienes siempre me brindaron la fuerza para seguir adelante en mi camino profesional.

Finalmente, a mi compañera de vida, quien fue mi apoyo durante el desarrollo de la presente investigación.

Agradecimientos

Agradezco principalmente a Dios, por brindarme salud, conocimiento y paciencia para poder avanzar en cada etapa de mi vida.

A la Universidad Nacional Mayor de San Marcos, especialmente a la facultad de Ingeniería Industrial, por permitirme concluir con esta etapa profesional.

Finalmente, agradecer al Ingeniero Willy Calsina, por su apoyo durante el desarrollo de la tesis.

RESUMEN

En la presente tesis se desarrolla la implementación de un sistema de gestión de continuidad del negocio (SGCN) basado en la ISO 22301, en una entidad financiera, con el objetivo de demostrar que este sistema permitirá a la organización estar preparada para hacer frente a situaciones adversas que pongan en riesgo la consecución de sus objetivos.

En el capítulo I, se describe la importancia y la necesidad que tienen las empresas en la actualidad de contar con un SGCN, asimismo se describen los objetivos del presente trabajo de investigación.

En la siguiente etapa (capítulo II), se describen los antecedentes que ha tenido el tema de continuidad del negocio y como ha ido evolucionando a lo largo del tiempo; por otra parte, se detallan conceptos claves, tales como análisis de impacto, gestión de riesgos, auditoría, entre otros. Es importante mencionar que estos conceptos deben ser de conocimiento para poder implementar este sistema.

La etapa del diseño de la investigación (capítulo IV), considera tres sub etapas, en la primera se realiza un análisis pre implementación, que consiste en identificar las brechas que tiene la organización con respecto al tema de continuidad del negocio; en la segunda sub etapa se realiza la implementación propiamente, que consiste en realizar un análisis de impacto para identificar los principales productos de la organización, los procesos que soportan estos productos, las principales amenazas que podrían ocasionar la paralización temporal o permanente de las operaciones de las organización y los planes para mitigar dichas amenazas; y finalmente la tercera sub etapa está referida a la mejora continua, que consiste en realizar evaluaciones periódicas tales como auditorías, que permitan identificar debilidades en el sistema, con el objetivo de corregirlas oportunamente.

Finalmente, en los dos últimos capítulos (V y VI), se muestran los resultados obtenidos luego de la implementación del SGCN en la organización, asimismo se describen algunas recomendaciones que pueden ser tomadas para estudios posteriores.

Palabras clave: ISO 22301, continuidad del negocio, análisis de impacto, amenazas.

ABSTRACT

This thesis develops the implementation of a business continuity management system (SGCN) based on ISO 22301, in a financial institution, with the aim of demonstrating that this system will allow the organization to be prepared to deal with adverse situations that put at risk the achievement of their objectives.

Chapter I describes the importance and necessity that companies currently have of a SGCN, and also describes the objectives of this research work.

The next stage (chapter II), describes the background of business continuity and how it has evolved over time; On the other hand, key concepts are detailed, such as impact analysis, risk management, auditing, among others. t's important to know that these concepts must been known in order to implement this system.

The research design stage (chapter IV), considers three sub-stages, in the first it performs a pre-implementation analysis, which is to identify the gaps that the organization has respect to the business continuity issue; In the second sub-stage, the implementation is carried out, which is to perform an impact analysis to identify the organization main products, the processes that support these products, the main threats that could cause the temporary or permanent shutdown of organizational operations and plans to mitigate such threats; and finally, the third sub-stage is about continuous improvement, which consists of conducting regular assessments such as audits, to identify weaknesses in the system, with the aim of correcting them in a timely manner.

Finally, the last two chapters (V and VI), show the results obtained after the implementation of the SGCN in the organization, it also describes some recommendations that can be made for futher studies.

Keywords: ISO 22301, business continuity, impact analysis, threats.

ÍNDICE

INTRODUCCIÓN 1

I. PROBLEMA DE LA INVESTIGACIÓN 2

1.1 Descripción del problema 2

1.2 Definición del problema 3

1.2.1 Problema general 3

1.2.2 Problemas específicos 4

1.3 Justificación e importancia de la investigación 4

1.3.1 Justificación teórica 4

1.3.2 Justificación práctica 5

1.3.3 Justificación metodológica 6

1.4 Objetivos de la investigación 7

1.4.1 Objetivo general 7

1.4.2 Objetivos específicos 7

II. MARCO TEÓRICO 8

2.1 Antecedentes de la investigación 8

2.2 Antecedentes nacionales: 12

2.3 Antecedentes internacionales: 14

2.4 Bases teóricas 15

2.4.1 ISO 15

2.4.2 ISO 22301 15

2.4.3 Continuidad del negocio 17

2.4.4 Análisis de impacto (BIA) 18

2.4.5 Gestión de riesgos 19

2.4.6 Auditoría 20

2.5 Marco conceptual 21

III. FORMULACIÓN DE HIPÓTESIS 23

3.1 Hipótesis general 23

3.2 Hipótesis específicas 23

3.3 Variables 23

3.3.1 Variables dependientes: 23

3.3.2 Variables independientes: 23

IV. DISEÑO DE LA INVESTIGACIÓN 28

4.1 Tipo de investigación 28

4.2 Diseño de la investigación 28
4.3 Población y muestra 29
4.4 Técnicas e instrumentos de recolección de datos 29
4.5 Técnicas de procesamiento y análisis de datos 30
4.6 Diagnóstico situacional de la entidad financiera 30
4.6.1 Análisis de la compañía 30
4.6.2 Estructura organizacional 30
4.6.3 Ubicación e infraestructura 32
4.6.4 Análisis gap del sistema de gestión de continuidad del negocio de la organización 32
4.7 Análisis de impacto al negocio – BIA (Business Impact Analysis) 37
4.7.1 Identificación de los productos y servicios críticos – BIA estratégico 37
4.7.2 Identificación de procesos críticos – BIA táctico 43
4.7.3 Identificación de actividades asociadas a procesos críticos - BIA operativo 46
4.7.4 Determinación de RTO, RPO, MTPD 58
4.8 Gestión de riesgos 98
4.8.1 Identificación de amenazas 100
4.8.2 Identificación de componentes de afectación 102
4.8.3 Identificación de Controles 103
4.8.4 Evaluación de Riesgos 107
4.8.5 Tratamiento de los riesgos de Continuidad 110
4.9 Evaluación y selección de estrategias 119
4.10 Planes de continuidad 128
4.10.1 Plan de respuesta de emergencia 130
4.10.2 Plan de gestión de crisis 131
4.10.3 Plan de comunicación 133
4.10.4 Plan de recuperación de desastres 134
4.10.5 Plan de capacitación 135
4.10.6 Plan de pruebas 136
4.11 Pruebas del sistema de gestión de continuidad 138
4.12 Auditoría del sistema de gestión de continuidad del negocio 142
V. ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS 162
5.1 Presentación de resultados 162
5.2 Contrastación de hipótesis 163
5.2.1 Contrastación de hipótesis general 164
5.2.2 Contrastación de hipótesis específica 1 164

5.2.3 Contrastación de hipótesis específica 2 165
5.2.4 Contrastación de hipótesis específica 3 165
5.2.5 Contrastación de hipótesis específica 4 166
5.3 Discusión de resultados 166
VI. CONCLUSIONES Y RECOMENDACIONES 167
6.1 Conclusiones 167
6.2 Recomendaciones 168
BIBLIOGRAFÍA 170
ANEXOS 174

ÍNDICE DE TABLAS

Tabla 1: Normas de la SBS y su relación con la Gestión de Continuidad del Negocio 4
Tabla 2: Ejemplos de sedes afectadas producto de algún evento disruptivo - 2017..... 5
Tabla 3: Descripción del modelo PDCA aplicado al SGCN 16
Tabla 4: Matriz de consistencia 25
Tabla 5: Cumplimiento de la ISO 22301 – Circular SBS G-139 (Fase inicial) 33
Tabla 6: Tipos de Impacto para la identificación de productos y servicios críticos 39
Tabla 7: Nivel de impacto según categoría 39
Tabla 8: Ponderación según tipo de productos 42
Tabla 9: Utilidad que generan los productos 43
Tabla 10: Procesos relacionados a los productos sobre los cuales se aplicará el SGCN 44
Tabla 11: Criticidad según proceso asociados a los productos créditos y ahorros 45
Tabla 12: Resumen de los procesos críticos, sus actividades relacionadas y procesos soporte 49
Tabla 13: Nivel de impacto definido para identificación del MTPD..... 59
Tabla 14: MTPD para el proceso de evaluación de clientes 62
Tabla 15: Detalle de registros vitales – Proceso evaluación de clientes 63
Tabla 16: Interrelación de los factores clave en el proceso de evaluación de clientes 65
Tabla 17: MTPD para el proceso de aprobación de créditos..... 68
Tabla 18: Detalle de registros vitales – Proceso aprobación de créditos 69
Tabla 19: Interrelación de los factores clave en el proceso de aprobación de créditos 71
Tabla 20: MTPD para el proceso de aprobación de desembolso de créditos 73
Tabla 21: Detalle de registros vitales – Proceso desembolso de créditos 74
Tabla 22: interrelación de los factores clave en el proceso de desembolso de créditos..... 76
Tabla 23: Identificación del MTPD del proceso de fondeo por depósito al público 78
Tabla 24: MTPD para el proceso de fondeo por depósitos del público 81
Tabla 25: Detalle de registros vitales – Proceso de fondeo por depósito al público 82
Tabla 26: Interrelación de los factores clave en el proceso de fondeo por depósito del público 84
Tabla 27: MTPD para el proceso de gestión de canales de atención 88
Tabla 28: Detalle de registros vitales – Proceso de gestión de canales de atención 89
Tabla 29: Interrelación de los factores clave en el proceso de gestión de canales de atención91
Tabla 30: MTPD para el proceso de atención al cliente 94

Tabla 31: Detalle de registros vitales – Proceso de atención al cliente 95
Tabla 32: Interrelación de los factores clave en el proceso de atención al cliente 96
Tabla 33: Principales riesgos de la organización 101
Tabla 34: Ejemplo de evaluación de riesgos 102
Tabla 35: Ejemplo de aplicación de controles en riesgos 104
Tabla 36: Ejemplo de aplicación de tributos de medición de la efectividad del control 106
Tabla 37: Parámetros de probabilidad 107
Tabla 38: Parámetros de impacto 107
Tabla 39: Descripción del nivel de criticidad 109
Tabla 40: Nivel de criticidad residual de los riesgos de continuidad identificados 111
Tabla 41: Tipos de estrategias 119
Tabla 42: Ventajas y desventajas de las estrategias 120
Tabla 43: Estrategias para los riesgos identificados 124
Tabla 44: Tiempos de recuperación objetivo real, proyectado y tiempo de recuperación tolerable 139
Tabla 45: Programa de Trabajo – Auditoría al Sistema de Gestión de Continuidad del Negocio 143
Tabla 46: Relación de procesos críticos y productos críticos 162
Tabla 47: Incremento del cumplimiento de la ISO 22301 163

ÍNDICE DE FIGURAS

Figura 1: Evolución de los lineamientos referidos a Continuidad del Negocio 9
Figura 2: Modelo PDCA aplicado al SGCN 15
Figura 3: Relación de apartados de la norma ISO 22301 17
Figura 4: Etapas de un análisis BIA 18
Figura 5: Proceso de recuperación de un SGCN 19
Figura 6: Fases del sistema de gestión de riesgos 20
Figura 7: Nivel de cumplimiento de la ISO 22301 35
Figura 8: Mapa de calor de Riesgos 108
Figura 9: Gráfico de costos de implementación de estrategias de continuidad vs tiempo de recuperación 122
Figura 10: Cronología de activación de los planes de continuidad 129
Figura 11: Comparación de tiempo de RTO y MTPD 140
Figura 12: Comparación del nivel de cumplimiento de la norma ISO 22301 – Antes y después de la implementación 161

INTRODUCCIÓN

En un mercado cada vez más competitivo, las empresas deben tener como principal preocupación al cliente. Debido a ello es que las organizaciones deben asegurar que el producto o servicio final que se brindará, se encuentre disponible en todo momento. Sin embargo, existen diferentes factores que pueden afectar las operaciones de dichas empresas, poniendo en riesgo la entrega de estos productos.

A pesar que muchas organizaciones son conscientes de la existencia de riesgos que pueden afectar el desarrollo normal de sus operaciones, no suelen contar planes que permitan hacer frente a estas amenazas. Esto debido a que no se toma conciencia del impacto que podría generar en caso suceda un evento disruptivo.

Como parte de esta necesidad es que surgió la norma ISO 22301, relacionada al tema de gestión de continuidad del negocio.

Un sistema de gestión de continuidad basado en la norma ISO 22301, tiene como finalidad demostrar que la organización se encuentra preparada para brindar sus productos o servicios ante eventos disruptivos, generando que el cliente no se vea afectado, y asegurando que la organización pueda sobreponerse a eventos adversos.

La presente tesis estudia la implementación de un sistema de gestión de continuidad basado en la ISO 22301 en una entidad financiera; sin embargo, cabe destacar que este sistema puede ser aplicado en cualquier otra entidad dedicada a diferentes rubros.

I. PROBLEMA DE LA INVESTIGACIÓN

1.1 Descripción del problema

En un mercado cada vez más competitivo, es importante que las empresas (independientemente del rubro al que pertenezcan) puedan garantizar la operatividad de sus procesos y servicios a las diferentes partes interesadas (stakeholders); sin embargo, existen situaciones tanto externas como internas que podrían conllevar a interrumpir el funcionamiento regular de las operaciones, y es en estos casos en los que se observa la importancia de contar con un sistema de gestión de continuidad.

En un estudio realizado por la Comunidad Andina (2010), se indica que Perú se encuentra en uno de los países de mayor vulnerabilidad ante situaciones de desastres naturales tales como sismos, inundaciones y otros; sin embargo a pesar de conocer estos aspectos, la mayor parte de las empresas no suelen optar por una certificación en temas relacionados a continuidad del negocio, como por ejemplo la certificación en la norma internacional ISO 22301; tal es el caso que hasta el año 2015, sólo cuatro empresas se encontraban en proceso de certificación respecto al tema en mención, según destacó Pedro Fernández, director General de AENOR Perú, para diario Gestión.[1]

Uno de los fenómenos naturales más conocidos y padecidos por el territorio peruano es el denominado fenómeno del niño costero, el cual es un fenómeno climático que se presenta con frecuencia irregular de entre tres y ocho años[2]; y cuyo acontecimiento suele generar grandes pérdidas. Recientemente, en el año 2017, Perú sufrió nuevamente el golpe de este fenómeno, y aunque ya se contaba con experiencias como las que acontecieron en los años 1997 y 1998, se demostró que tanto las entidades del sector público como privado no se encontraban preparadas para hacer frente a estas situaciones. El sector financiero no fue ajeno al impacto de este evento, tal es el caso que grandes empresas como el BBVA Continental y Scotiabank presentaron

[1] Gestión (2015). *Para la certificación de ISO, el Perú es un "mercado muy reducido"*. Recuperado de https://gestion.pe/economia/empresas/certificacion-iso-peru-mercado-reducido-93181

[2] Wikipedia (2019). *Niño costero de 2016 – 2017*. Recuperado de https://es.wikipedia.org/wiki/Ni%C3%B1o_costero_de_2016-2017

interrupción en sus operaciones debido a caída en las redes y comunicaciones, así como también debido al difícil acceso a las instalaciones como consecuencia de vías dañadas[3].

Por otra parte, si bien los desastres naturales son situaciones que pueden afectar directamente a la continuidad de las operaciones de una organización; existen otros eventos que también pueden ocasionar la paralización de dichas operaciones, como por ejemplo un simple corte de energía eléctrica, desabastecimiento de agua, manifestaciones, y otros similares.
En ese contexto; las empresas deben encontrarse preparadas para responder de manera efectiva a las situaciones adversas que se presenten y que por diferentes motivos no le permitan continuar brindando productos o servicios al consumidor.

Considerando lo descrito, es que surge la necesidad que una organización cuente con un Sistema de Gestión de Continuidad del Negocios (SGCN), cuyo objetivo es brindar servicios de forma aceptable a sus clientes.

En la presente tesis, se va desarrollar la propuesta de un SGCN para una entidad financiera, haciendo énfasis en la gestión de riesgos de continuidad, a efectos de desarrollar estrategias que permitan responder adecuadamente a los diferentes escenarios planteados. Finalmente se planteará un programa de auditoría que permita verificar el cumplimiento del sistema, y el nivel de madurez del mismo.

1.2 Definición del problema

1.2.1 Problema general

- ¿Cómo influye la implementación de un Sistema de Gestión de Continuidad del Negocio basado en la norma ISO 22301 en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos?

[3] Salas, L. (2017). *Así sufren las empresas el impacto de El Niño en el norte*. Recuperado de https://elcomercio.pe/economia/dia-1/sufren-empresas-impacto-nino-norte-407191

1.2.2 Problemas específicos

- ¿Cómo influye el análisis de impacto al negocio de la norma ISO 22301 en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos?
- ¿Cómo influye la gestión de riesgos de la norma ISO 22301 en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos?
- ¿Cómo influye el establecimiento de planes de continuidad de la norma ISO 22301 en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos?
- ¿Cómo influye la ejecución de auditorías de la norma ISO 22301 en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos?

1.3 Justificación e importancia de la investigación

1.3.1 Justificación teórica

El presente estudio, se desarrolla en una entidad financiera, la cual se encuentra regulada por las disposiciones establecidas por la Superintendencia de Banca, Seguros y AFP (SBS); que exige entre otros aspectos, el cumplimiento de las siguientes normas, Circular Nº G-139-2009, Circular Nº G-140-2009, y la Resolución Nº 2116-2009 (ver Tabla 1).

Tabla 1: Normas de la SBS y su relación con la Gestión de Continuidad del Negocio

Norma	Objetivo	Relación con la Gestión de Continuidad del Negocio
Circular Nº G-139-2009	Norma referida a la implementación de un Sistema de Gestión de Continuidad del Negocio.	En su artículo 8º, establece las fases a desarrollar en un SGCN.
Circular Nº G-140-2009	Norma que hace referencia a la implementación de un Sistema de Gestión de Seguridad de la Información.	En su artículo 5.7º, destaca la importancia de los procedimientos de respaldo; y que estos deben ser coherentes con la estrategia de

		continuidad de la empresa.
Resolución Nº 2116-2009	Norma que establece los aspectos necesarios para la gestión del Riesgo Operacional.	En su artículo 13º, establece que las empresas deben implementar un SGCN, a fin de contar con respuestas efectivas para continuar con las operatividad de las operaciones de forma razonable.

Fuente: Circular SBS Nº G-139, Circular Nº G-140-2009, Resolución Nº 2116-2009. Elaboración Propia.

Uno de los objetivos de la presente tesis, es demostrar la importancia de contar con un sistema de Gestión de Continuidad del Negocios, basado en la norma internacional ISO 22301, el cual permitirá a la entidad financiera contar con los procedimientos necesarios para dar respuesta a posibles eventos que pudieran interrumpir el desarrollo regular de las operaciones de la empresa; y al mismo tiempo dar cumplimiento a las exigencias establecidas por la SBS.

1.3.2 Justificación práctica

El presente estudio, se ha desarrollado en una entidad financiera, la cual cuenta con cuarenta (40) establecimientos en todo el país.

En razón que la empresa está orientada de forma específica al sector de las microfinanzas, sus establecimientos se encuentran ubicados en zonas rurales. Dichas sedes, debido a la geografía y otros factores sociales propios de la zona en que se encuentran localizadas, están expuestas a posibles eventos, como son desastres naturales, indisponibilidad de los servicios, robos, manifestaciones y otros; aspectos que no han sido analizados mediante una correcta evaluación de riesgos a fin de desarrollar estrategias y planes de recuperación adecuados (Ver Tabla 2).

Tabla 2: Ejemplos de sedes afectadas producto de algún evento disruptivo - 2017

Evento	Sedes afectadas	Consecuencia
Fenómeno del Niño Costero	Agencia A1, ubicada en la región	Esta sede no pudo operar durante 03 días. No se activaron los procedimientos de continuidad.

Evento	Sedes afectadas	Consecuencia
	de Trujillo.	
	Agencia A2, ubicada en Huachipa.	Debido al fenómeno, se presentaros huaycos, y deslizamientos que afectaron la operatividad de la sede.
Desabastecimiento de servicios	Oficina Especial A3, ubicada en Jicamarca.	Presenta desabastecimiento frecuente de los servicios básicos (agua y luz); esto impide de forma recurrente el desarrollo regular de las operaciones.
Manifestaciones	Agencia A4, ubicada en Lima Cercado.	Debido a manifestaciones que se presentaron cerca a la sede se vio forzada a cerrar sus instalaciones.
Delincuencia	Agencia A5, ubicada en San Juan de Lurigancho	La empresa se vio forzada a cerrar la agencia ubicada en San Juan de Lurigancho, debido a que en una sede de otra entidad bancaria y ubicada contiguamente se presentó un asalto.

Fuente: Información del departamento de operaciones de la organización

Elaboración Propia

Por otra parte, cabe indicar que, la calificación otorgada por la Oficina de Auditoría de la empresa objeto de estudio respecto a la gestión de continuidad del negocio en los dos últimos años (2016 y 2017) ha sido 'inefectiva' – la peor calificación resultado de una auditoría; aspecto que deja en evidencia la inadecuada gestión de continuidad.

Es importante indicar que si bien la empresa en estudio cuenta con ciertos procedimientos para dar solución a eventos disruptivos; no cuenta con un SGCN; el cual no solo señala que se debe contar con planes de continuidad, sino que describe la importancia de contar con una cultura de continuidad, que debe ser practicada desde los trabajadores, hasta los niveles más altos de la organización, la alta dirección.

1.3.3 Justificación metodológica

Un sistema de gestión se puede entender como una herramienta que ayuda a

utilizar los recursos de una empresa en forma eficiente, disminuyendo costos e incrementando su productividad. En ese sentido un sistema de gestión de continuidad del negocio se puede entender como una herramienta que otorga a una empresa la capacidad para seguir brindando los productos y servicios a sus clientes - a un nivel aceptable - luego de haber sufrido un incidente que haya interrumpido sus operaciones.

En ese sentido con la presente tesis, se pretende evidenciar que la norma internacional ISO 22301, es la más adecuada para implementar un sistema de Gestión de Continuidad del Negocio, independientemente del sector al que corresponda la institución.

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Implementar un sistema de gestión de continuidad del negocio basado en la norma ISO 22301 para evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos.

1.4.2 Objetivos específicos

- Implementar el análisis de impacto al negocio de la norma ISO 22301 para evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos
- Implementar la gestión de riesgos de la norma ISO 22301 parar evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos
- Establecer planes de continuidad de la norma ISO 22301 para evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos
- Ejecutar auditorías de la norma ISO 22301 para evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos

II. MARCO TEÓRICO

2.1 Antecedentes de la investigación

Uno de los principales conceptos referidos a la continuidad del negocio, es el de 'disaster recovery' (recuperación de desastres por su traducción al español). Este concepto tiene sus orígenes en las décadas de los años setenta. En aquella época, los centros de cómputo eran considerados como 'puntos únicos de falla' (Single points of failure – SPFO), y en ese sentido se desarrollaron servicios a través de los cuales diversos proveedores ofrecían acceso compartido a entornos de recuperación informática, conocidos como centro de respaldos. Ya en los años ochenta y noventa, este servicio adquirió mayor énfasis en el mercado, haciendo notar a las organizaciones que entre más dependencia presentaran respecto a la tecnología, mayor podría ser el impacto, en tanto no cuenten con sistemas de recuperación de infraestructura e información[4]. Es a partir de este tipo de situaciones que las empresas analizan que las interrupciones que afecten a las tecnologías de información, pueden generar pérdidas significativas, dada la fuerte dependencia de la misma.

En 1994, se crea el BCI (Business Continuity Institute)[5], organización que actualmente cuenta con más de ocho mil miembros[6], y que promueve orientación y las mejoras prácticas en temas de continuidad del negocio. En 1995 se publica uno de los lineamientos más antiguos referidos a continuidad, como es el caso de la NFPA 1600, herramienta que brinda criterios orientados sobre todo a la gestión de emergencias y desastres. Unos años más tarde, en 1997, el DRII (Disaster recovery institute international) difunde las 'Prácticas profesionales para la gestión del negocio'[5]. En el 2003, el BSI (British Standard Institute), publica la PAS 56, guía que brindó principios y mejores prácticas respecto a la gestión de continuidad del negocio[5]. A pesar de los lineamientos establecidos, es recién en el 2006, que se publica el BS 25999-1, estándar que describe un modelo para la gestión de continuidad del negocio; y un año después, se publicaría el primer estándar certificable y auditable, el BS 25999-25.

Finalmente, en el 2012, se publicaría el estándar ISO 22301:2012 (Seguridad de la

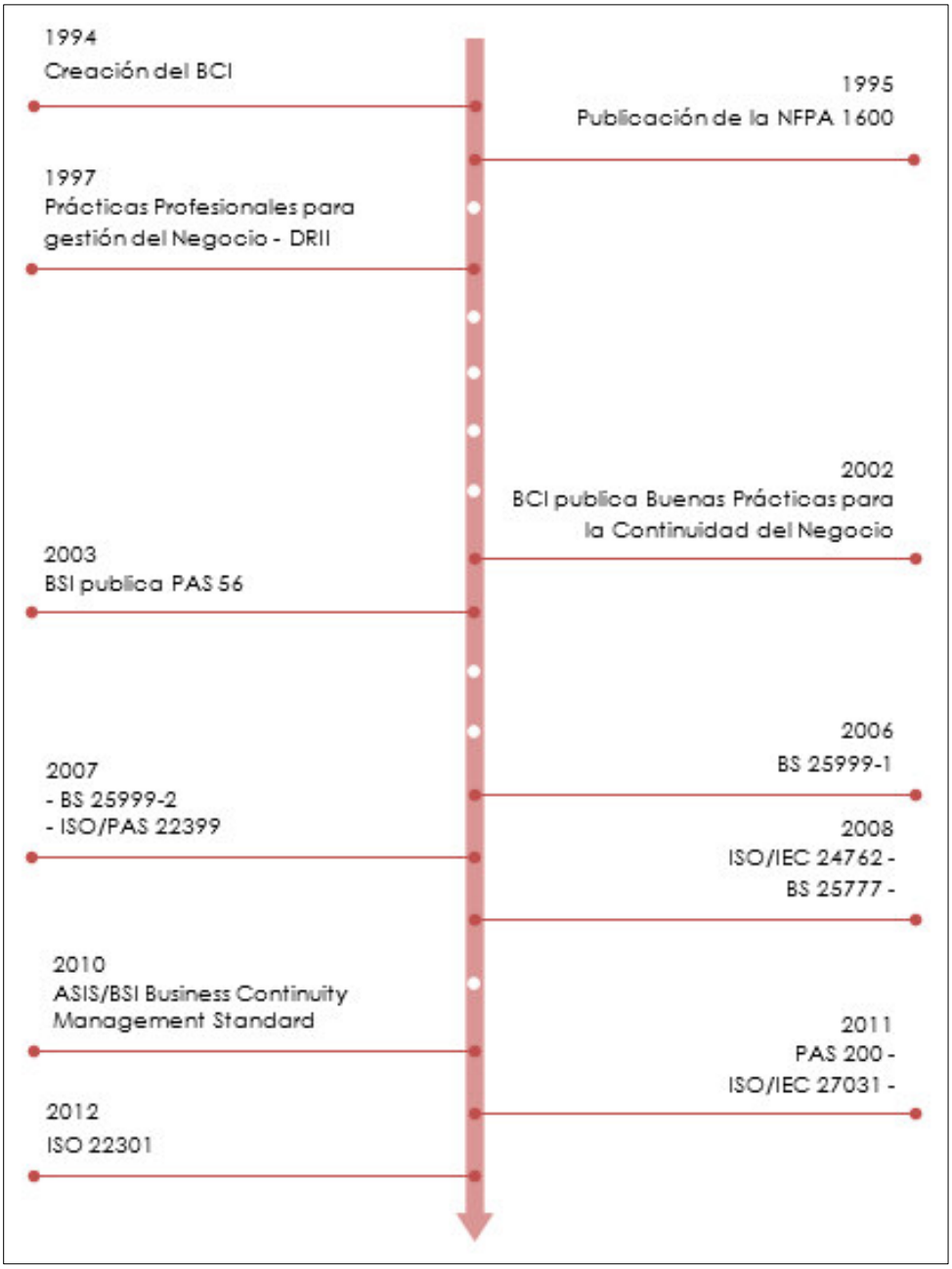
[4] Garay, J. (2012). *Antecedentes históricos de la continuidad del negocio*. Recuperado de http://businesscontinuity-pe.blogspot.com/2012/07/antecedentes-historicos-de-la.html

[5] Quevedo, J. (2012). *Revisión de modelos de gestión de continuidad del negocio*. Recuperado de revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/download/5620/4877

[6] BCI (2019).

Sociedad: Sistemas de Continuidad del Negocio), el cual sería auditable y certificable, y que reemplazaría al BS 25999-27. En la figura 1 se puede apreciar la evolución de los aspectos referidos a continuidad del negocio.

Figura 1: Evolución de los lineamientos referidos a Continuidad del Negocio



Fuente: Servat, A (2012). *Nuevo estándar internacional en continuidad del negocio ISO 22301-2012*. GESTIÓN.

[7] Servat, A (2012). *Nuevo estándar internacional en continuidad del negocio ISO 22301-2012*. GESTIÓN. Recuperado de https://www.gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf

Tal como se ha podido apreciar, el tema de continuidad del negocio no es nuevo; a lo largo del tiempo se han ido desarrollando diferentes lineamientos que han permitido establecer criterios necesarios para un adecuado SGCN.

Haciendo énfasis en el ámbito local; si bien Perú "es un mercado muy reducido para las certificaciones ISO"[8] (Pedro Fernández, Director general de Aenor Perú (2015)); el tema de continuidad, ha ido tomando mayor énfasis; entre lo que se puede destacar la normas que ha establecido la SBS) - tales como la circular Nº G-139-2009 - así como la creación del instituto de continuidad del negocio (Continuam) en febrero del 2016.
A continuación, se presentan dos casos, uno de ellos (Lehman Brothers) que evidencia el éxito de una empresa respecto a la eficiente respuesta ante situaciones adversas; y otro (Bembos) que evidencia las consecuencias de no realizar un adecuado análisis respecto a los escenarios en los que se podría encontrar una empresa y que pudieran afectar la continuidad de sus operaciones:

Caso Lehman Brothers

El 11 de setiembre de 2001, aconteció en Estados Unidos uno de los atentados más catastróficos que la historia ha podido presenciar. Estos actos fueron ejecutados por personas que formaban parte de la red yihadista Al Qaeda; ocasionando la muerte de aproximadamente 3 (tres) mil personas, y la destrucción de edificios del 'World Trade Center', entre los que destacan las 'torres gemelas'[9].
Como consecuencia de este atentado, aproximadamente catorce (14) mil empresas dejaron de brindar servicios de forma permanente, en razón que no pudieron responder de forma efectiva ante dicha situación.

Situación diferente fue la que presentó Lehman Brothers Holding Inc. – empresa dedicada a brindar servicios financieros y cuyo cierre se produjo en septiembre del 2008 – una de las compañías que se encontraban en la torre uno del World Trade Center. Esta empresa contaba con un plan de continuidad, y con una sede alterna

[8] Gestión (2015). *Para la certificación de ISO, el Perú es un "mercado muy reducido"*. Recuperado de https://gestion.pe/economia/empresas/certificacion-iso-peru-mercado-reducido-93181

[9] Wikipedia (2019). *Atentados del 11 de setiembre de 2001*. Recuperado de https://es.wikipedia.org/wiki/Atentados_del_11_de_septiembre_de_2001

totalmente equipada, en la cual se replicaba toda la información de forma automática; lo que permitía contar con un backup en línea.

El plan de continuidad de Lehman Brothers fue activado de forma oportuna por el Director de Tecnología de Información; este hecho permitió que el mismo día (11 de septiembre 2001) el departamento de Economía pueda continuar con sus actividades de gestión de fondos; asimismo un día después del atentado (12 de septiembre 2001) la empresa ya contaba con aproximadamente cuatrocientos (400) empleados preparados para poder gestionar acciones y fondos cuando la Bolsa de Nueva York reabra sus puertas.

El Director de Tecnología de Información, señaló que el éxito de la continuidad operativa de la empresa se debió gracias al diseño de las redes y comunicaciones; así como a la rápida respuesta al plan de continuidad.

En febrero del 2002, la empresa Gartner Group (hoy en día Gartner Inc – empresa dedicada a actividades de consultoría e investigación relacionadas a las tecnologías de información), "reveló que aproximadamente el 85% de las grandes empresas tenía planes de recuperación ante desastres; no obstante sólo el 25 % contaban con un plan integrado y de mayor alcance (el cual no se encuentre orientado solamente al resguardo de la información, sino que considere también a la participación del personal, infraestructura tecnológica y otros); señalando que sólo el 10% (de ese 25%) tenía planes actualizados"[10].

Caso Bembos

El 22 de febrero del 2015, Digesa - Dirección General de Salud Ambiental, decide cerrar la fábrica de alimentos Bimbo, en razón que identificó proveedores con registro sanitario equivocados.

Esta situación generó como consecuencia el desabastecimiento de grandes cadenas de comida rápida (fast food), como es el caso de Bembos; compañía que no pudo prever este aspecto - la indisponibilidad del proveedor de su principal producto - de forma oportuna; lo que implicó no poder brindar sus productos de forma regular; llegando a ofrecer inclusive hamburguesas sin pan, como estrategia imprevista ante el evidente

[10] Sanchez, F. (2002). *Network World. Bajo el "Efecto 11 de septiembre". Planes de continuidad del negocio*. Recuperado de https://www.networkworld.es/archive/bajo-el-efecto-11-de-septiembre-planes-de-continuidad-del-negocio

desabastecimiento. Este inconveniente fue resuelto tres días después (25 de febrero 2015) de haberse presentado el cierre de su principal proveedor.

Este tipo de situaciones generan un gran impacto en las empresas; desde cuantiosas pérdidas económicas debido a la reducción en sus ventas, así como el impacto negativo reputacional ante la disconformidad de sus clientes; quizá este último podría considerarse de mayor gravedad, en razón del amplio alcance con el cual se difunden los acontecimientos a través de redes sociales hoy en día.

Se debe tener en cuenta que un sistema de gestión de continuidad no debe considerar sólo los aspectos internos y cómo estos podrían afectar a las operaciones de la empresa, sino también factores externos, como el ambiente geográfico, político, proveedores y otros; ya que la afectación o cambios de alguno de estos factores, pueden impactar significativamente en la continuidad de las operaciones de una empresa; aspecto que claramente no fue estudiado, ni considerado como posible escenario a efectos de mitigar el riesgo, por parte de la cadena Bembos.
Por otra parte, se debe mencionar que existen estudios (tesis) respecto al tema de continuidad del negocio, los cuales fueron determinantes para el desarrollo de la presente tesis. Entre estos estudios, se pueden destacar los siguientes:

2.2 Antecedentes nacionales:

- En la tesis de nombre 'Modelo de un sistema de gestión de continuidad del negocio para microfinanciera basado en la ISO/IEC 22301 y en la circular G-139-2009 de la SBS', propuesta por los autores Leonard Soto y Karina Céspedes, se presenta una metodología que permitirá hacer frente a eventos disruptivos en una empresa dedicada al sector micro financiero; sin embargo, es importante destacar que a pesar que esta metodología se basa en la ISO 22301 no se identificó los productos críticos de la organización, sino más bien, se inicia con el análisis a partir de los procesos de la empresa.

  Cabe indicar que es de vital importancia, como primer paso de la metodología, identificar los productos y/o servicios que brinda una organización, y sobre ellos implementar el sistema de gestión de continuidad del negocio; ya que se debe velar

por la entrega de estos productos y servicios hacia el cliente.

En la tesis en mención, se concluye que la norma internacional ISO 22301, es aplicable a cualquier entidad financiera, y asimismo puede ser adaptable según el requerimiento de la organización.

Adicionalmente, se aprecia que se analiza el cumplimiento de la ISO 22301 y de la circular SBS Nº G-139 de forma individual; este aspecto se toma como un input, ya que, en la presente tesis, se integrará y verificará que el cumplimiento de la ISO 22301 conlleva implícitamente al cumplimiento de la circular SBS Nº G-139.

- En la tesis de nombre 'Modelo de análisis de impacto en el negocio para el desarrollo de la continuidad de negocio aplicable a empresas del sector financiero', escrita por el autor Carmen Castillo, se presenta una metodología para el análisis de impacto al negocio, sin embargo, se inicia dicho análisis a partir de los procesos de la organización, y posteriormente se analizan los productos asociados a los procesos críticos. Tal como se mencionó en el punto anterior, el análisis para la implementación de un sistema de continuidad del negocio, debe partir desde la identificación de productos y servicios críticos, y sobre ellos asociar los procesos.

  Cabe indicar también que el estudio realizado por el autor, Carmen Castillo, no está orientado a la implementación de un sistema de gestión en su totalidad, sino sólo al análisis de impacto (BIA); este aspecto se toma como input para la presente tesis, ya que se realizará también el análisis de riesgo y un programa de auditoría para la implementación completa del sistema de gestión.

  La tesis en mención concluye indicando que el cumplimiento del sistema de gestión de continuidad basado en BS-25966, conlleva al cumplimiento de la circular G-139, establecida por la SBS.

- El objetivo principal de un sistema de gestión de continuidad del negocio es reanudar todas las operaciones que permitan continuar con la entrega de productos y/o servicios al cliente. Considerando que, en su mayor parte, los procesos para el otorgamiento de un producto o servicio requiere el soporte de procesos tecnológicos, es que en las tesis 'Seguridad y Plan de contingencia en centros de informática', escrita por el autor Carmen Peña, y 'Plan de contingencias y de recuperación de desastres', escrita por el autor Carlos Barragán; se desarrollan

planes orientados a reanudar y recuperar los procesos de tecnología de información, con el objetivo de brindar soporte a los demás procesos críticos y así poder brindar los producto y/o servicios que requiera la organización.

Este aspecto se ha considerado como input para la presente tesis, en razón que se desarrollará una etapa orientada a establecer planes de continuidad, que permitan responder adecuadamente a eventos adversos.

La tesis en mención concluye indicando que la principal preocupación de las organizaciones es velar por la operatividad del hardware, software y datos de los sistemas de información que soportan sus procesos, debido a ello considera como aspecto fundamental el tema de continuidad.

Finalmente, se debe considerar la importancia de contar con un sistema de continuidad del negocio, y no sólo con planes aislados; situación – que según la empresa Ernst & Young – presenta el 52% de organizaciones del Perú (según su estudio de gobierno, gestión de riesgos y auditoría en el Perú 2016-2017) [11].

2.3 Antecedentes internacionales:

- Diseño y propuesta de implementación de un plan de continuidad del negocio aplicable a los hospitales en la ciudad de Bogotá (J. Angel, H. Velasco, 2014).

  La tesis establece la implementación de planes de continuidad, para lo cual plantea el análisis de los riesgos que pueden afectar la continuidad de las operaciones de la organización. En la investigación se concluye que el tema de continuidad no es de amplio conocimiento, y tampoco de aplicación en los hospitales de la ciudad de Bogotá.

- Plan de continuidad del negocio basado en servicios en la nube para el área de tecnología (G. Castillo, 2017).

  Esta tesis plantea como solución, desarrollar un plan de continuidad del negocio, considerando como estrategia contar con un sitio en la nube que permita a la organización recuperar sus principales procesos desde este ambiente.

[11] Ernst & Young (2017). *Promoviendo el desarrollo de una cultura de prevención. Estudio de gobierno, gestión de riesgos y auditoría interna en el Perú 2016-17.* Recuperado de http://www.ey.com/pe/es/issues/ey-promoviendo-desarrollo-cultura-prevencion

La tesis concluye indicando que un servicio de computación en la nube podría considerarse como una de las estrategias más adecuadas para las organizaciones, teniendo en cuenta los continuos avances tecnológicos, además del ahorro de gastos en temas de infraestructura y equipos que ello implica.

2.4 Bases teóricas

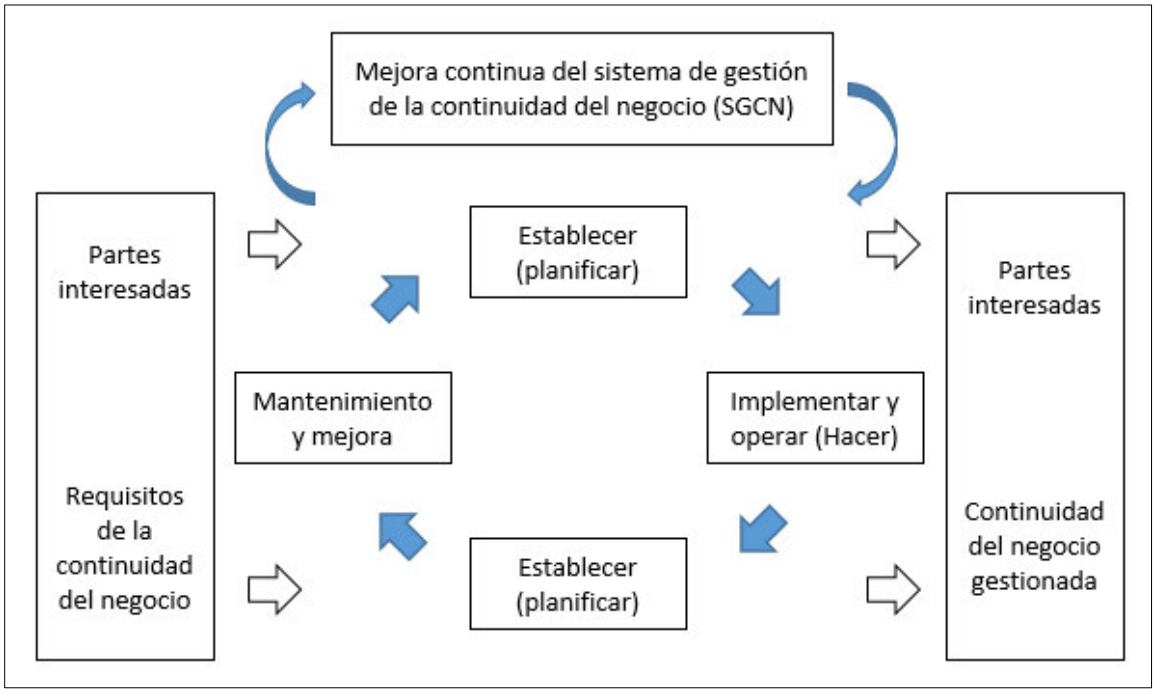
2.4.1 ISO

La ISO, cuya descripción en inglés significa International Organization for Standardization, es una organización que tiene por objetivo la creación de estándares internaciones para las diferentes empresas.

2.4.2 ISO 22301

Se puede describir a la norma ISO 22301, como un estándar que tiene por objetivo describir los requisitos necesarios para la implementación de un sistema de Gestión de Continuidad del Negocio (SGCN). Esta norma toma como referencia el modelo de mejora continua, PDCA por sus siglas en inglés (Plan, Do, Check, Act).

Figura 2: Modelo PDCA aplicado al SGCN



Fuente: Norma internacional ISO 22301 – numeral 0.2

Tabla 3: Descripción del modelo PDCA aplicado al SGCN

P	Plan (Planificar)	En esta etapa se establece la política de continuidad del negocio, así como sus objetivos, controles, procesos y procedimientos acordes con las políticas y objetivos de la organización.
D	Do (Hacer)	Esta etapa consiste en aplicar la política, controles, procesos y procedimientos de continuidad.
C	Check (Verificar)	Supervisar la efectividad del sistema de gestión considerando los objetivos y política establecidos. Proceder con informar a los niveles correspondientes, y proponer medidas para su corrección y mejora.
A	Act (Actuar)	Mantener y mejorar el SGCN, considerando el resultado de la revisión de la Dirección de la organización.

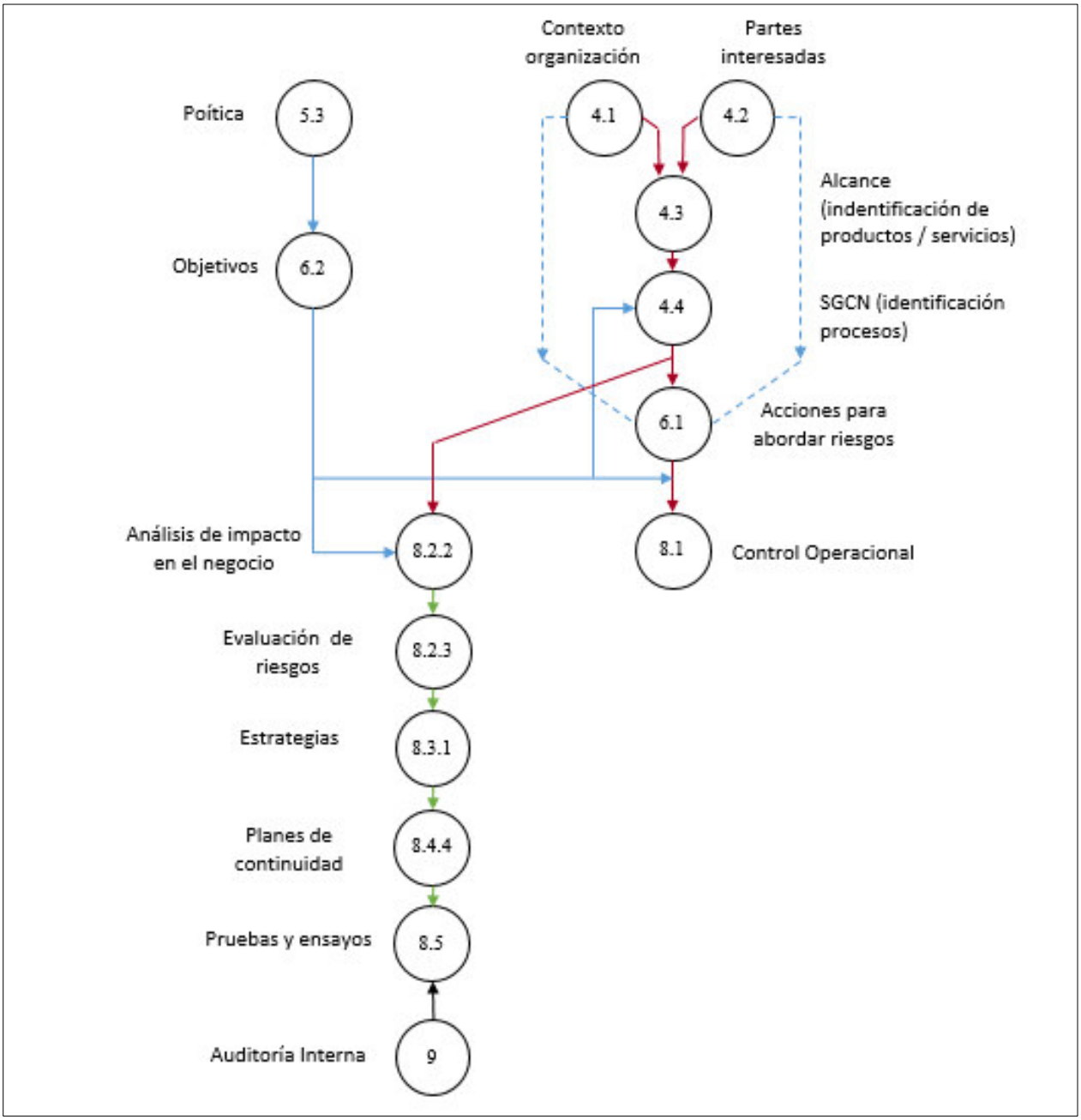
Fuente: Norma internacional ISO 22301 – numeral 0.2

Por otra parte, se debe tener en cuenta que cada apartado de la norma ISO 22301, se encuentra relacionado, y en su conjunto conlleva a la implementación del SGCN (ver figura 2.3).

En la figura 3, se puede apreciar que la norma ISO 22301, inicia con identificar el contexto de la organización (apartado 4.1) y las partes interesadas (apartado 4.2); posteriormente determina los productos y servicios críticos (apartado 4.3), para luego identificar los procesos asociados a estos productos (apartado 4.4). Como siguiente paso, se debe realizar el análisis de impacto al negocio (apartado 8.2.2), luego realizar la evaluación de riesgos (apartado 8.2.3), y posteriormente determinar las estrategias (apartado 8.3.1), planes de continuidad (apartado 8.4.4), y plan de pruebas (apartado 8.5).

Finalmente se debe considerar en la última etapa un sistema de monitoreo como es el caso de auditorías (apartado 9).

Figura 3: Relación de apartados de la norma ISO 22301



Fuente: ISO 22301 – Elaboración propia

2.4.3 Continuidad del negocio

El estándar ISO 22301, define a la continuidad del negocio, como la "*capacidad de la organización para continuar realizando la entrega de productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo*"[12].

Por otra parte, se puede entender que la gestión de continuidad del negocio, es un

[12] ISO 22301 (2012).

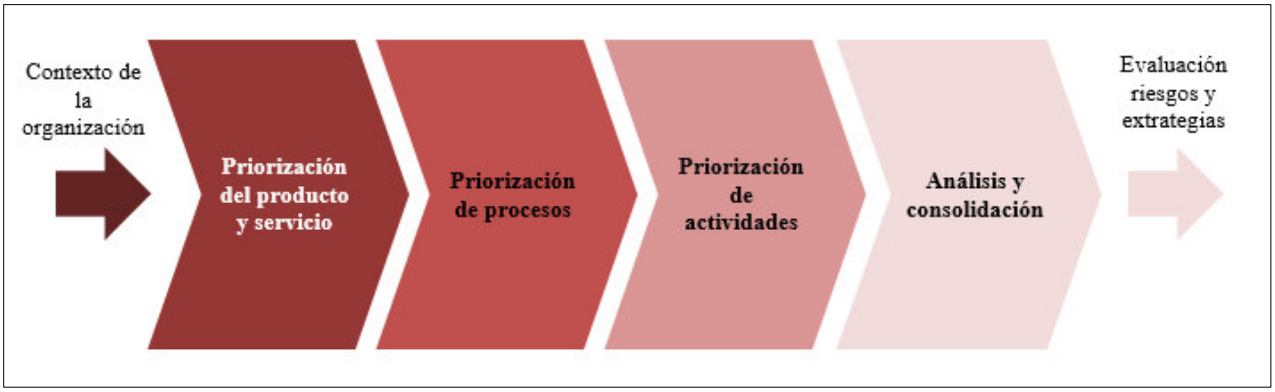
proceso a través del cual se identifican los riesgos a los cuales está propensa una organización, y el impacto que dichos riesgos podrían ocasionar en caso de interrumpir de forma significativa las operaciones de la empresa; esto a efectos de establecer medidas y lineamientos que permitan aumentar la capacidad de respuesta y resiliencia de la institución a fin de hacer frente a dichos eventos, salvaguardar los intereses de la empresa, así como disminuir posibles pérdidas.

Es importante destacar que la continuidad está directamente relacionada al producto o servicio que brinda una organización, para lo cual es crucial identificar los procesos y actividades críticas necesarias para poder brindar dicho producto o servicio; a fin de establecer planes adecuados que permitan reanudar sus procesos y actividades.

2.4.4 Análisis de impacto (BIA)

El análisis de impacto al negocio, según describen John W. Rittinghouse, y James F. Ransome en su libro Business Continuity and Disaster Recovery for Infosec Managers, es un proceso orientado a identificar funciones críticas para el negocio, y las pérdidas y efectos que se ocasionarían en caso éstos no se encuentren disponibles. En la figura 4 se puede apreciar las etapas de un proceso de análisis de impacto al negocio.

Figura 4: Etapas de un análisis BIA



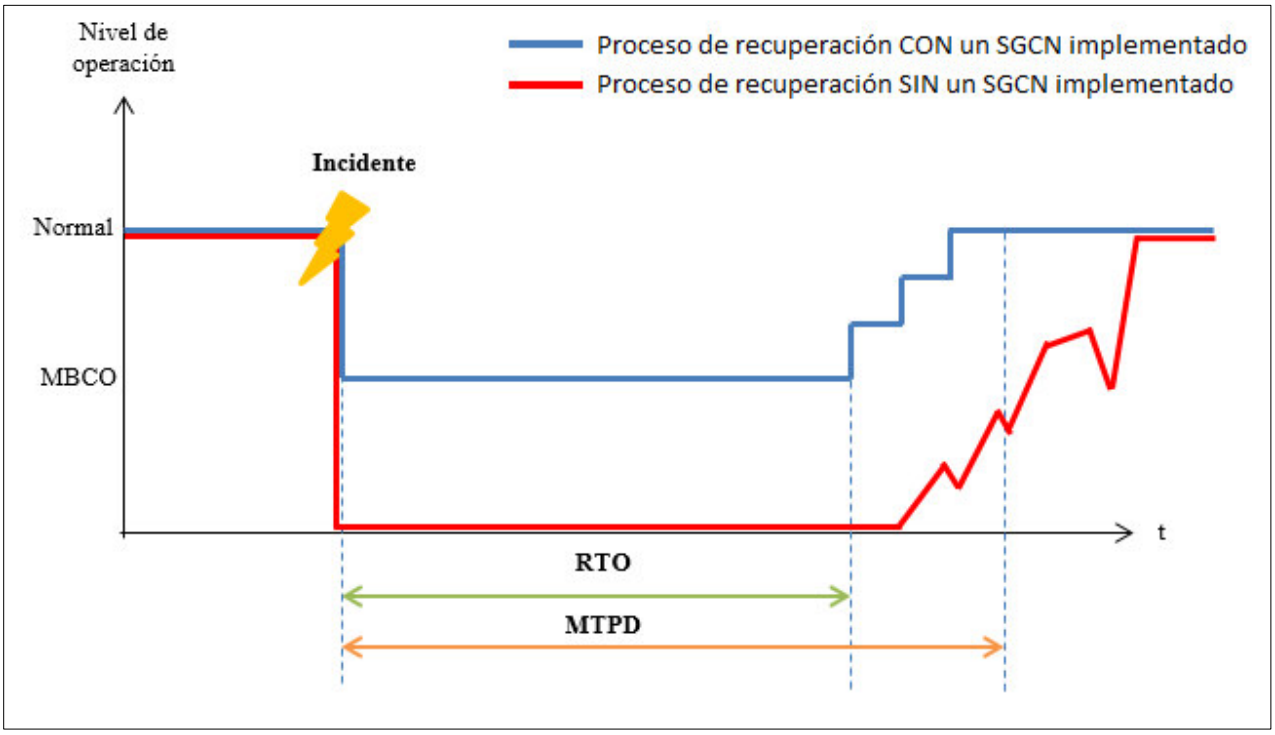
Fuente: Elaboración propia

Como parte del análisis de impacto al negocio, se determina el tiempo de recuperación (RTO) por cada proceso crítico, teniendo en cuenta el periodo máximo de interrupción tolerable (MTPD), y los niveles mínimos aceptables

(MBCO) para el otorgamiento de productos/servicios.

En la figura 5 se puede apreciar, que un proceso de recuperación en una organización que cuenta con un sistema de gestión de continuidad del negocio, es más rápido que el proceso de recuperación de una organización que no cuenta con este sistema. Incluso, se puede apreciar que la recuperación a un estado normal (situación que presenta la organización antes de acontecer el incidente) en las organizaciones que no tienen un SGCN, generalmente ocurre superado el periodo máximo de interrupción tolerable (MTPD), lo cual implica pérdidas para la empresa.

Figura 5: Proceso de recuperación de un SGCN



Fuente: Elaboración propia

2.4.5 Gestión de riesgos

El marco de control interno COSO, entiende al riesgo, como la posibilidad que ocurra un evento que puede impactar negativamente y poner en riesgo la consecución de objetivos de la organización13.

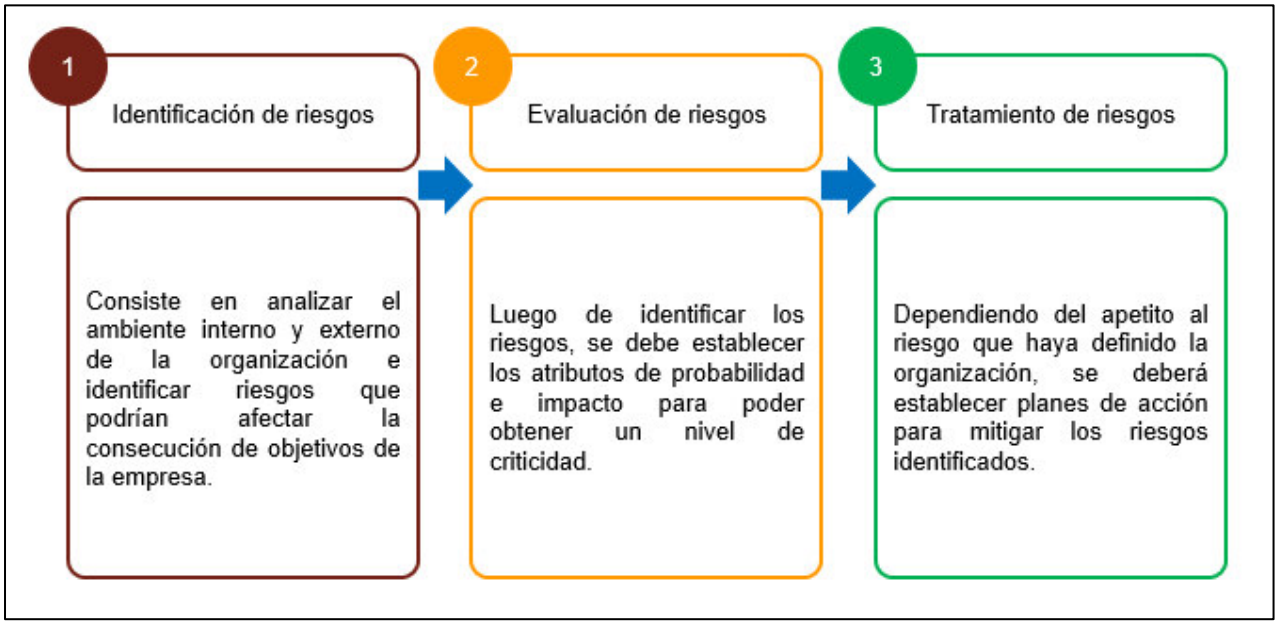
La gestión de riesgos, inicia con la fase de identificación de riesgos, posteriormente

[13] Everson et al. (2013). Control Interno – Marco Integrado.

con la evaluación y finaliza con el tratamiento de los riesgos.

Para ello debe tenerse en cuenta términos como, riesgo inherente, riesgo residual, control, probabilidad e impacto; términos serán desarrollados con mayor profundidad en el numeral 4.8 de la presente tesis.

Figura 6: Fases del sistema de gestión de riesgos



Fuente: Elaboración propia

2.4.6 Auditoría

La norma internacional ISO 19011, define a la auditoría como un proceso mediante el cual se verifica el cumplimiento de la organización respecto al tema evaluado. Se podría clasificar a la auditoría en tres tipos:

- Auditorías de primera parte: Son aquellas evaluaciones realizadas por la Gerencia de Auditoría Interna. Esta Gerencia forma parte de la organización, pero debe contar con el principio de independencia para la ejecución de sus labores.
- Auditorías de segunda parte: Son aquellas evaluaciones realizadas por las partes interesadas, tales como clientes, o sus representantes.
- Auditorías de tercera parte: Son evaluaciones realizadas de forma independiente por entidades externas, que podrían ser consultoras o entidades reguladoras.

2.5 Marco conceptual

En el presente estudio se hace uso de diversos términos, los cuales se desarrollarán a lo largo de la esta tesis, sin embargo, a continuación, se describen los más importantes:

Análisis de Impacto:

Proceso que permitirá identificar los productos y/o servicios críticos para la organización, teniendo en cuenta el tiempo máximo que pueden permanecer inoperativos antes de empezar a generar pérdidas.

RTO

Iniciales de recovery time objective, cuya traducción en español es, tiempo de recuperación objetivo. Este valor, representa el tiempo en el cual la organización esperar que sus operaciones vuelvan a la normalidad, luego de haber sucedido un evento negativo.

RPO

Iniciales de recovery point objective, cuya traducción en español es, punto de recuperación objetivo. Este valor representa a la cantidad de información que la empresa está dispuesta a perder ante un evento disruptivo.

MTPD

Iniciales de máximum tolerable period of disruption, cuya traducción en español es, periodo máximo de interrupción tolerable. Este valor, representa el tiempo que la empresa puede tener inoperativos sus productos o servicios, antes que la inoperatividad de los mismos comience a generar pérdidas graves para la organización.

Apetito de riesgo

El Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, define al apetito de riesgo como el nivel de riesgo que la organización puede aceptar a efectos de poder conseguir sus objetivos.

Reanudación

Entiéndase, para la presente tesis, que la reanudación está referida a poner en marcha, bajo niveles aceptables, las operaciones orientadas a brindar un producto o servicio

crítico, luego de un evento disruptivo.

Restauración

Entiéndase, para la presente tesis, que la restauración está referida a poner en marcha, bajo niveles normales, las operaciones orientas a brindar un producto o servicio crítico, luego de un evento disruptivo. Entiéndase por niveles normales el desarrollo de las operaciones en situaciones no afectadas por eventos adversos.

III. FORMULACIÓN DE HIPÓTESIS

3.1 Hipótesis general

La implementación de un sistema de gestión de continuidad del negocio basado en la norma ISO 22301 evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

3.2 Hipótesis específicas

- El análisis de impacto al negocio sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas
- La implementación de la gestión de riesgos de la norma ISO 22301 sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas
- Establecer planes de continuidad del negocio sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas
- La ejecución de auditorías sí evidencian la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

3.3 Variables

En la presente tesis las variables a utilizar son las siguientes:

3.3.1 Variables dependientes:

- Capacidad de la organización para continuar brindando sus productos y/o servicios
- Identificación de productos, servicios y procesos críticos
- Riesgos que pueden afectar la continuidad de las operaciones
- Establecer procedimientos de recuperación de procesos críticos
- Nivel de cumplimiento de la norma ISO 22301

3.3.2 Variables independientes:

- Sistema de gestión de continuidad del negocio basado en la norma ISO 22301
- Análisis de impacto al negocio (BIA)
- Gestión de riesgos

- Planes de continuidad del negocio
- Auditorías internas

(Los indicadores se pueden apreciar en la matriz de consistencia que puede ver en la tabla 4)

Tabla 4: Matriz de consistencia

Formulación del problema	Objetivos	Hipótesis	Variables	Indicadores	Metodología
Problema General	**Objetivo General**	**Hipótesis General**	**Variable dependiente**		
¿Cómo influye la implementación de un Sistema de Gestión de Continuidad del Negocio basado en la norma ISO 22301 en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos?	Implementar un sistema de gestión de continuidad del negocio basado en la norma ISO 22301 para evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos	La implementación de un sistema de gestión de continuidad del negocio basado en la norma ISO 22301 evidencia la capacidad de la organización para continuar brindando productos y/o servicios antes situaciones disruptivas	Capacidad de la organización para continuar brindando sus productos y/o servicios **Variable independiente** Sistema de gestión de continuidad del negocio basado en la norma ISO 22301	Número de pruebas efectivas de planes de continuidad (Número de planes efectivos / número de planes totales)	**Investigación**: Descriptiva
Problema Específico 1	**Objetivo Específico 1**	**Hipótesis Específica 1**	**Variable dependiente**	% de productos críticos	
¿Cómo influye el análisis de impacto al negocio de la norma ISO 22301 en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos?	Implementar el análisis de impacto al negocio de la norma ISO 22301 para evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos	El análisis de impacto al negocio sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas	Identificación de productos, servicios y procesos críticos **Variable independiente** Análisis de impacto al negocio (BIA)	(productos críticos / total de productos de la organización) % de procesos críticos (procesos críticos / total de procesos de la	**Diseño de investigación**: No experimental

Formulación del problema	Objetivos	Hipótesis	Variables	Indicadores	Metodología
				organización)	
Problema Específico 2	**Objetivo Específico 2**	**Hipótesis Específica 2**	**Variable dependiente**	% de controles estrategias y controles implementados para los riesgos (número de controles / total de riesgos)	**Población**: Todos los productos de la empresa Financiera **Instrumentos**: Microsfot Excel, ACL **Técnicas**: observación, entrevistas,
¿Cómo influye la gestión de riesgos de la norma ISO 22301 en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos?	Implementar la gestión de riesgos de la norma ISO 22301 parar evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos	La implementación de la gestión de riesgos de la norma ISO 22301 sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas	Riesgos que pueden afectar la continuidad de las operaciones **Variable independiente** Gestión de riesgos		
Problema Específico 3	**Objetivo Específico 3**	**Hipótesis Específica 3**	**Variable dependiente**	% de planes de recuperación por proceso (número de planes de recuperación / procesos críticos de la organización)	
¿Cómo influye el establecimiento de planes de continuidad de la norma ISO 22301 en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos?	Establecer planes de continuidad de la norma ISO 22301 para evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos	Establecer planes de continuidad del negocio sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas	Establecer procedimientos de recuperación de procesos críticos **Variable independiente** Planes de continuidad del negocio		
Problema Específico 4	**Objetivo Específico 4**	**Hipótesis Específica 4**	**Variable dependiente**	% cumplimiento del sistema de	

Formulación del problema	Objetivos	Hipótesis	Variables	Indicadores	Metodología
¿Cómo influye la ejecución de auditorías de la norma ISO 22301 en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos?	Ejecutar auditorías de la norma ISO 22301 para evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante eventos disruptivos	La ejecución de auditorías sí evidencian la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas	Nivel de cumplimiento de la norma ISO 22301 **Variable independiente** Auditorías internas	gestión de continuidad (ítems implementados / total de ítems de la norma ISO 22301)	diagrama de flujos

IV. DISEÑO DE LA INVESTIGACIÓN

4.1 Tipo de investigación

El tipo de investigación se considera como exploratorio y descriptivo. Exploratorio, ya que son pocos los estudios y casos de éxito presentados respecto a la implementación de Normas ISO 22301 en entidades financieras en el Perú. Por otra parte, se considera también de tipo descriptivo, en razón que se ha recolectado información, que permita tomar conocimiento de la situación de la organización a evaluar, con el objetivo de analizarlos y poder describir el problema investigado, y la solución brindada.

4.2 Diseño de la investigación

El diseño de la investigación será no experimental, principalmente porque el presente estudio está basado en la observación, así como en el análisis de los factores internos y externos que afectan a la continuidad de las operaciones de la empresa. No es posible manipular la variable independiente.

Por otra parte, se considera que el diseño de la investigación es también transversal, en razón que los datos son recolectados al momento de implementar la ISO 22301 (por lo tanto, se considera un momento específico).

31660624

Las actividades necesarias para la implementación de un sistema de Gestión de Continuidad del Negocio bajo la ISO 22301, en la entidad financiera, son las siguientes:

1. Se realiza un análisis situacional respecto al sistema de gestión de continuidad del negocio que tiene la entidad financiera objeto de estudio, identificando las brechas pendientes por cubrir respecto a la ISO 22301.
2. Según la ISO 22301, la 'continuidad' se aplica sobre un producto o servicio, en ese sentido se procede a identificar el universo de productos y servicios que brinda la entidad financiera, y sobre los cuales se desea aplicar 'continuidad'.
3. Habiendo identificado los productos y/o servicios sobre los cuales se aplicará continuidad, se debe proceder con el análisis de impacto al negocio (BIA), para lo cual se deberá determinar los procesos críticos, y actividades críticas respectivamente.
4. Identificar los riesgos a los cuales se encuentra expuesta la organización. Cabe

indicar que los riesgos deben ser aquellos que atenten contra la continuidad de las operaciones de la organización.

5. Establecer estrategias que permitan mitigar los riesgos identificados, y poder brindar los productos o servicios a un nivel aceptable.
6. Establecer los planes de continuidad.
7. Desarrollar los planes de pruebas.
8. Desarrollar un modelo de auditoría para el cumplimiento y mejora continua del SGCN.

4.3 Población y muestra

El SGCN, debe ser aplicado sobre los productos y servicios que la entidad considere conveniente (Según la ISO 22301), para ello deberá aplicar ciertos criterios que le permitan determinar adecuadamente dichos productos.

Considerando lo anteriormente descrito, se entiende que la población comprende a todos los productos y servicios que brinda la entidad financiera, y para la determinación de la muestra se utilizará la metodología según tipos de impacto descrita en la Norma Técnica ISO/TS 22317.

4.4 Técnicas e instrumentos de recolección de datos

Considerando que toda técnica de recolección de datos tiene como objetivo recabar información que permita un adecuado análisis; a efectos de poder implementar un sistema de gestión de continuidad del negocio, se han considerado las siguientes técnicas: observación, entrevistas, diagrama de flujos.

La observación es el método fundamental de obtención de datos de la realidad, toda vez que consiste en obtener información mediante la percepción intencionada y selectiva, ilustrada e interpretativa de un objeto o de un fenómeno determinado‖. Para el método de observación se debe de tener en cuenta todas las actitudes, conductas, manifestaciones entre otros, que pueden variar a pesar de ser el mismo escenario aparentemente. Se tiene dos tipos de observación, la sistemática o estructurada y la no sistemático o no estructurada. La entrevista se utiliza para recabar información en forma verbal, a través de las preguntas que propone el investigador o entrevistador. Consiste en una conversación entre una o más personas en la cual uno es el

entrevistador y el otro u otros son los entrevistados o informantes claves. Los diagramas de flujo son una representación pictórica de los pasos en proceso. Útil para determinar cómo funciona realmente el proceso para producir un resultado. Los diagramas de flujo se pueden aplicar a cualquier aspecto del proceso desde el flujo de materiales hasta los pasos para hacer la venta u ofrecer un producto.

4.5 Técnicas de procesamiento y análisis de datos

La información será organizada principalmente en la herramienta de cálculo Microsoft Excel, por otra parte, los diagramas de flujos serán diseñados con la herramienta Microsoft Visio; finalmente toda información que represente grandes volúmenes de datos – tales como cartera de créditos, bases de datos históricas de incidencias o similares – será trabajada con la herramienta de análisis de datos ACL (software para análisis de datos utilizado por las áreas de auditoría interna).

4.6 Diagnóstico situacional de la entidad financiera

4.6.1 Análisis de la compañía

La organización objeto de estudio, es una entidad que cuenta (CIIU 6430) con muchos años en el mercado y está dedicada, desde sus inicios, a las microfinanzas. Debido a su naturaleza, esta entidad se encuentra regulada según las disposiciones establecidas por la SBS (según la Ley Nº 26702 – Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros).

4.6.2 Estructura organizacional

La entidad principalmente se encuentra segregada en siete gerencias (incluida la Gerencia General), y dos unidades de cumplimiento, las cuales cumplen las siguientes funciones (ver anexo A):

- Gerencia de Auditoría: Órgano que desempeña un rol independiente a la gestión y cuya función principal es la evaluación del diseño, alcance y funcionamiento del sistema de control interno de la institución.
- Gerencia General: Órgano responsable de ejecutar y hacer cumplir los acuerdos

adoptados por la Junta General de Accionistas de Directorio; así como supervisar la veracidad de la información proporcionada al Directorio, a la SBS, y demás instituciones públicas y privadas que lo soliciten.

- Gerencia de Riesgos: Encargado de la identificación y administración de todos los riesgos financieros (riesgo de crédito) y no financieros (riesgos operacionales y de seguridad de la información) que enfrenta la entidad; teniendo en cuenta las normas establecidas por los órganos de control, supervisión y regulación correspondientes.
- Gerencia de Negocios: Órgano encargado de colocar y captar fondos disponibles en sus diferentes modalidades de créditos y ahorros, utilizando criterios racionales en la evaluación y procurando obtener la máxima rentabilidad al menor costo posible.
- Gerencia Legal: Gerencia encargada de asegurar que las acciones legales, judiciales y de asesoría sean atendidas de forma oportuna, eficiente y eficaz cautelando los intereses institucionales; además de velar por la recuperación efectiva de la cartera de créditos en situación de judicial y de castigo.
- Gerencia de Administración: Gerencia encargada de organizar, dirigir, ejecutar, coordinar y supervisar las actividades relacionadas con los procesos de gestión de personal, logística de recursos, tecnología de la información, normativa interna, mejora de los procesos y seguridad física de la institución.
- Gerencia de Finanzas y Operaciones: Órgano encargado de planear, organizar y ejecutar las actividades relacionadas con la administración y control de los procesos operativos propios de la institución; y controlar diariamente la posición y la integridad de los recursos financieros y el cumplimiento de los límites de liquidez y cobertura de seguros; además de velar por el desarrollo adecuado de las actividades contables y de la captación de ahorros u otros depósitos provenientes de sus clientes.
- Unidad de Prevención de Lavado de Activos: Tiene como objetivo principal vigilar el cumplimiento del sistema de prevención de lavado de activos y del financiamiento del terrorismo de la institución.
- Unidad de Atención al Usuario: Esta unidad es la encargada de velar por el adecuado funcionamiento del sistema de atención al usuario; velando por la implementación y el cumplimiento de las normas vigentes en materia de protección al consumidor, transparencia de la información, atención al usuario y

demás disposiciones establecidas por la Superintendencia de Banca, Seguros y AFP.

4.6.3 Ubicación e infraestructura

La entidad objeto de estudio, debido a la actividad que desarrolla – proveer servicios crediticios generalmente a sectores que se encuentran excluidos del sistema financiero tradicional – establece sus agencias, principalmente, en zonas rurales, a efectos de poder tener mayor alcance del mercado en su mercado objetivo.

La entidad financiera cuenta con 53 tipos de establecimientos, 04 oficinas informativas, 08 locales compartidos, 13 oficinas especiales, y 28 agencias.

- Oficinas Informativas: Establecimientos en los cuales sólo se brinda información respecto a los servicios financieros que tiene la entidad a disposición de sus clientes.
- Locales Compartidos: Son establecimientos que pertenecen al Banco de la Nación, y con los cuales se ha establecido un convenio a efectos que la entidad en estudio) pueda brindar sus servicios en dichos lugares.
- Oficinas Especiales: Establecimientos en los cuales la entidad ofrece sus servicios financieros (principalmente otorgamiento de créditos, y captaciones de fondos del público), sin embargo, debido al número de las operaciones que realiza no pueden ser considerados dentro de la categoría de 'agencias'.
- Agencias: Establecimientos en los cuales la entidad ofrece sus servicios financieros, referidos al otorgamiento de créditos y captaciones de fondos. Se diferencia de una oficina especial, debido a que una agencia posee un gran número de operaciones.

Las ubicaciones de los establecimientos se pueden apreciar en el anexo B.

4.6.4 Análisis gap del sistema de gestión de continuidad del negocio de la organización

En esta etapa se debe indicar el nivel de cumplimiento que tiene la organización respecto a la norma ISO 22301. Cabe indicar que al cumplir los apartados

establecidos en la norma ISO 22301, implícitamente se cumple la norma SBS G-Nº 139.

Tabla 5: Cumplimiento de la ISO 22301 – Circular SBS G-139 (Fase inicial)

Norma ISO 22301		**Norma SBS G- Nº 139**	**Nivel de cumplimiento: (0) No cumple, (1) Cumple Parcialmente, (2) Cumple**
4. Contexto de la organización		- **Artículo 8º (8.1)** - Entendimiento de la Organización (Considera análisis de impacto y evaluación de riesgos)	Puntaje de cumplimiento: 1.5
4.1 Entendimiento de la organización y de su contexto	2		
4.2 Entendimiento de las necesidades y expectativas de las partes interesadas	2		
4.3 Determinación del campo de aplicación del sistema de gestión de la continuidad del negocio	0		
4.4 Sistema de gestión de la continuidad del negocio	2		
5. Liderazgo		- **Artículo 4º** - Responsabilidad del Directorio - **Artículo 5º** - Responsabilidad de la Gerencia - **Artículo 6º** - Responsabilidad de la unidad de riesgos - **Artículo 7º** - Función de la continuidad del negocio	Puntaje de cumplimiento: 1.5
5.1 Liderazgo y compromiso	2		
5.2 Compromiso de la dirección	2		
5.3 Política	1		
5.4 Funciones, responsabilidades y autoridad en la organización	1		
6. Planificación			Puntaje de cumplimiento:

Norma ISO 22301		Norma SBS G- Nº 139	Nivel de cumplimiento: (0) No cumple, (1) Cumple Parcialmente, (2) Cumple
6.1 Acciones para cubrir riesgos y oportunidades	1		1.5
6.2 Objetivos de continuidad del negocio y planes para conseguirlos	2		
7. Apoyo		- **Artículo 9º** - Documentación sustentatoria	Puntaje de cumplimiento: 1.2
7.1 Recursos	1		
7.2 Competencia	1		
7.3 Concienciación	2		
7.4 Comunicación	1		
7.5 Información documentada	1		
8. Operación		- **Artículo 8º (8.2)** - Entendimiento de la Organización (Considera selección de estrategia de continuidad, y la ejecución de pruebas)	Puntaje de cumplimiento: 1.2
8.1 Planificación y control operacional	2		
8.2 Análisis de impacto en el negocio y apreciación del riesgo	1		
8.3 Estrategia de continuidad del negocio	1		
8.4 Establecimiento e implantación de procedimientos de continuidad del negocio	1		
8.5 Pruebas y ensayos	1		
9. Evaluación y medición del rendimiento		- **Artículo 10º** - Cambios significativos - **Artículo 11º** - Auditoría	Puntaje de cumplimiento: 1.3
9.1 Supervisión, medición,	1		

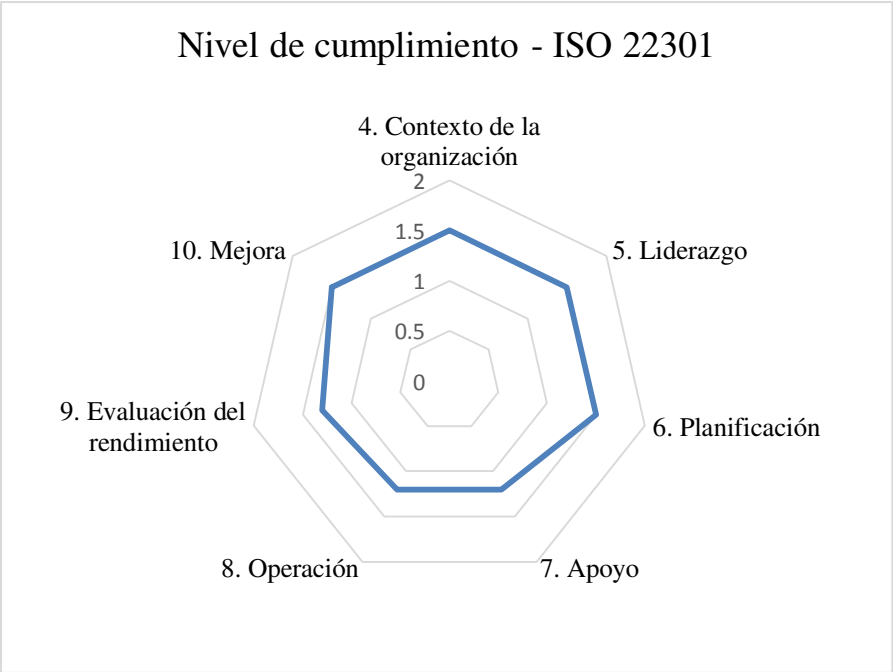
Norma ISO 22301		Norma SBS G- Nº 139	Nivel de cumplimiento: (0) No cumple, (1) Cumple Parcialmente, (2) Cumple
análisis y evaluación		interna	
9.2 Auditoría interna	2		
9.3 Revisión de la dirección	1		
10. Mejora			
10.1 No conformidad y acción correctora	1		Puntaje de cumplimiento: 1.5
10.2 Mejora continua	2		

Fuente: Elaboración propia

Para poder verificar el cumplimiento de cada uno de los aspectos descritos en el cuadro anterior, se consideraron los resultados obtenidos en la auditoría del periodo 2017.

En la figura 7, se puede apreciar el nivel de cumplimiento que tiene la organización con respecto a los apartados de la norma ISO 22301. Tal como se puede ver, existe un bajo nivel de cumplimiento con respecto a la norma en mención, esto debido a que no se contaba con un sistema de gestión de continuidad implementado.

Figura 7: Nivel de cumplimiento de la ISO 22301



Fuente: Elaboración propia

4.7 Análisis de impacto al negocio – BIA (Business Impact Analysis)

La etapa de análisis de impacto al negocio tiene por objetivo identificar los productos y/o servicios críticos para la organización, y sobre ellos determinar el tiempo límite que pueden estar inoperativos, es decir no brindar dichos productos/servicios al cliente; con el objetivo de establecer planes que permitan recuperar las operaciones en caso de eventos adversos.

4.7.1 Identificación de los productos y servicios críticos – BIA estratégico

Según lo establecido en la norma ISO 22301 – Sistema de Gestión de Continuidad del Negocio, se debe establecer los productos o servicios sobre los cuales se desee implementar el sistema de continuidad. Considerando ello se identificó el universo de productos y servicios financieros que brinda la entidad, agrupándolos de la siguiente forma:

- Remesas: Debido a que la entidad tiene convenios con la empresa Western Union, brinda servicio de remesas a nivel nacional e internacional, con el objetivo que los usuarios puedan enviar dinero dentro y fuera del país.
- Microseguros: Producto cuyo objetivo es proteger a los clientes contra riesgos específicos (muerte y desamparo familiar súbito), a cambio de pagos establecidos según convenios.
- SOAT (Seguro Obligatorio de Accidentes de Tránsito): Producto dirigido para todos aquellos clientes que cuentan con un vehículo; a través de este producto la entidad brinda un seguro cuyo objetivo es cubrir los riesgos de muerte y lesiones de aquellas victimas en accidentes de tránsito.
- Servicios de Giros Nacionales: Servicio a través del cual las personas pueden realizar envío de dinero en las diferentes agencias de la entidad, sin necesidad de contar con una cuenta de ahorros.
- Servicio de Recaudación: Servicio que permite al usuario, persona natural o persona jurídica, contar con un canal formal para realizar sus cobros. Entre los principales clientes de este tipo de servicio, se encuentran: instituciones educativas como colegios, institutos, universidades, empresas de transporte, de servicios públicos (electricidad, agua), entre otros.
- Tipo de Cambio: Consiste en brindar a los clientes un servicio a través del cual

pueden realizar el cambio de moneda extranjera en nacional, así como de moneda nacional en moneda extranjera.

- Recarga de Celulares: Servicio a través del cual la entidad ofrece a sus clientes la posibilidad de contar con saldo en sus equipos celulares.
- Créditos: Productos cuyo objetivo es brindar a los clientes préstamos de dinero, quienes en su calidad de deudores se comprometen a devolver la cantidad prestada en el tiempo y plazo según las condiciones que se hayan establecido.
  Bajo la modalidad de créditos, la entidad cuenta con diversos productos, que se diferencia en tasa y plazo, dependiendo del sector y el destino del crédito (crédito capital, crédito más, crédito activo fijo, crédito local, crédito fácil, crédito convenios, crédito construye, crédito vehículo, crédito autogas, crédito agropecuario, crédito de consumo directo, crédito descuento por planilla, crédito al personal, crédito profesional).
- Ahorros: Productos a través de los cuales la entidad realiza captación de fondos. Esta gama de productos tiene por objetivo custodiar de forma segura el dinero de los clientes, generando rentabilidad en forma de intereses teniendo en cuenta los plazos establecidos (ahorro simple, ahorro sueldo, ahorro infantil, ahorro mujer, ahorro programado, DPF interés periódico, DPF capital al vencimiento, ahorro CTS).

Luego de haber identificado el universo de productos y servicios que brinda la entidad financiera, se debe considerar los siguientes aspectos a efectos de determinar sobre qué productos aplicar el sistema de continuidad: i) criticidad de los productos o servicios según la metodología de impacto definida en la Norma de Especificación Técnica ISO/TS 22317 (Seguridad Social - Sistemas de Gestión de Continuidad de Negocios - Directrices para el análisis del impacto de negocios), ii) porcentaje de participación en las utilidades de los diversos productos, a efectos de determinar la importancia de los mismos para la entidad.

i) Según la Norma de Especificación Técnica ISO/TS 22317, la criticidad de un producto o servicio se determina en función al impacto que este genera para la empresa; considerando cinco tipos de impacto: financiero, reputación, legal y regulatorio, contractual, y finalmente objetivos del negocio.

Tabla 6: Tipos de Impacto para la identificación de productos y servicios críticos

Categorías de Impacto	Detalle
Financiero	Pérdidas financieras debido a multas, sanciones, pérdida de beneficios o disminuyen la cuota de Mercado
Reputación	Opinión negativa o daños a la marca
Legal y Regulatorio	Responsabilidades litigiosas y retiro de la licencia para el comercio
Contractual	Incumplimiento de contratos y obligaciones entre las organizaciones
Objetivos de negocios	Si no se cumplan los objetivos fijados o tomar ventaja de las oportunidades

Fuente: Norma Técnica ISO/TS 22317

Considerando ello, se desarrolló el siguiente nivel de ponderación para cada uno de los impactos:

Tabla 7: Nivel de impacto según categoría

Tipos de Impacto	Nivel de Impacto	Puntaje	Descripción
Financiero	Muy Bajo	1	Se considera un impacto de nivel muy bajo hasta S/ 1 mil
	Bajo	2	Se considera un impacto de nivel bajo hasta S/ 6 mil
	Medio	3	Se considera un impacto de nivel medio hasta S/ 30 mil
	Alto	4	Se considera un impacto de nivel alto hasta S/ 61 mil
	Muy alto	5	Se considera un impacto de nivel muy alto, mayor a S/ 61 mil
Reputacional	Muy Bajo	1	Se considera un nivel bajo si: • El impacto no afecta la imagen de la empresa. • Hasta 50 clientes afectados
	Bajo	2	Se considera un nivel bajo si: • El impacto afecta levemente la imagen de la empresa. • Hasta 200 clientes afectados
	Medio	3	Se considera un nivel bajo si:

Tipos de Impacto	Nivel de Impacto	Puntaje	Descripción
			• El impacto afecta la imagen de la empresa. Alcance a nivel distrital • Hasta 500 clientes afectados
	Alto	4	Se considera un nivel bajo si: • El impacto afecta en gran medida la imagen de la empresa. Alcance a nivel regional. • Hasta 2000 clientes afectados
	Muy alto	5	Se considera un nivel bajo si: • El impacto afecta gravemente la imagen de la empresa. Alcance a nivel internacional. • Más de 2000 clientes afectados
Legal o Regulatorio	Muy Bajo	1	Amonestaciones leves a la organización por parte de la SBS, SUNAT, MINTRA, u otros (Hasta 0,5 UIT)
	Bajo	2	Amonestaciones leves a la organización por parte de la SBS, SMV, INDECOPI, SUNAT, MINTRA, u otros. (Hasta 02 UIT)
	Medio	3	Amonestaciones leves a la organización por parte de la SBS, SMV, INDECOPI, SUNAT, MINTRA, u otros. (Hasta 08 UIT)
	Alto	4	• Amonestaciones graves a la organización por parte de la SBS, SMV, INDECOPI, SUNAT, MINTRA, u otros. • Suspensión de licencia de funcionamiento de la empresa. • Suspensión de la entrega de un producto o servicio de la empresa. (Hasta 16 UIT)
	Muy alto	5	• Amonestaciones graves a la organización por parte de la SBS, SMV, INDECOPI, SUNAT, MINTRA, u otros. • Cancelación de licencia de funcionamiento de la empresa. • Cancelación de la entrega de un producto o servicio de la

Tipos de Impacto	Nivel de Impacto	Puntaje	Descripción
			empresa. • Intervención de la empresa o sometimiento a régimen de vigilancia. (Mayor a 16 UIT)
Contractual	Muy Bajo	1	Incumplimiento de cláusulas contractuales con proveedores o clientes con posibilidad de demandas. (Hasta S/ 1 mil)
	Bajo	2	Incumplimiento de cláusulas contractuales con proveedores o clientes con posibilidad de demandas. (Hasta S/ 6 mil)
	Medio	3	Incumplimiento de cláusulas contractuales con proveedores o clientes con posibilidad de demandas. (Hasta S/ 30 mil)
	Alto	4	Incumplimiento de cláusulas contractuales con proveedores o clientes con posibilidad de demandas. (Hasta S/ 61 mil)
	Muy alto	5	Incumplimiento de cláusulas contractuales con proveedores o clientes con posibilidad de demandas. (Superior a S/ 61 mil)
Objetivos de Negocios	Muy Bajo	1	Incumplimiento en los objetivos que generen un impacto muy bajo en la empresa.
	Bajo	2	Incumplimiento en los objetivos que generen un impacto bajo en la empresa.
	Medio	3	Incumplimiento en los objetivos que generen un impacto medio en la empresa.
	Alto	4	Incumplimiento en los objetivos que generen un impacto alto en la empresa.
	Muy alto	5	Incumplimiento en los objetivos que generen un impacto muy alto en la empresa.

Fuente: Información de la Gerencia de Riesgos – Elaboración propia

Considerando los criterios previamente definidos, se identificó los productos y servicios críticos:

Tabla 8: Ponderación según tipo de productos

Producto / Servicio	Impacto					Puntaje
	Financiero	Reputación	Legal y Regulatorio	Contractual	Objetivos de Negocio	
Remesas	2	2	3	3	1	11
Microseguros	3	3	3	2	3	14
Soat	2	2	3	1	3	11
Giros Nacionales	2	2	3	0	1	08
Servicio de Recaudación	1	1	3	2	1	08
Tipo de Cambio	2	1	3	0	1	07
Créditos	4	5	5	0	4	18
Ahorros	5	5	5	5	5	25

Fuente: Evaluación realizada por la unidad de continuidad del negocio de la entidad.

Se considerarán como críticos aquellos productos que superen un puntaje de '15'. Cabe indicar que el límite de puntaje para considerar un producto como crítico, se ha obtenido de la siguiente forma:

a) Se determinará el promedio de la suma generada por los números del 01 al 05 (nivel de impacto).

$$\frac{(01 + 02 + 03 + 04 + 05)}{5} = 3$$

b) Se considerará como factor de multiplicación, el número de impactos que se han evaluado (05 tipos de impacto).

- Finalmente se procede a multiplicar los valores obtenidos en los pasos a) y b), generando que el límite que deben superar los productos para ser considerados como críticos, debe ser 15 (3 * 5).

ii) Se aplicará la ley de Pareto (80 - 20), determinando aquellos productos, que generen mayor utilidad para la empresa.

Tabla 9: Utilidad que generan los productos

Productos / Servicios	% Utilidad
Remesas	0.70 %
Microseguros	6.00 %
Soat	1.00 %
Servicios de Giros Nacionales	1.50 %
Servicio de Recaudación	1.10 %
Tipo de Cambio	0.05 %
Recarga de Celulares	0.05 %
Créditos	51.10 %
Ahorros	38.30 %
Total	**100.00 %**

Fuente: Departamento de Contabilidad

Como se puede apreciar en la tabla 8, más del 80% de la utilidad es generado principalmente por dos grupos de productos, que corresponden a Créditos y Ahorros.

Teniendo en cuenta la criticidad que tienen los productos identificados para la entidad, se establece que sobre dichos productos (créditos y ahorros) se aplicará el sistema de gestión de continuidad del negocio (SGCN).

4.7.2 Identificación de procesos críticos – BIA táctico

Luego de haber definido los productos sobre los cuales se aplicará el Sistema de Gestión de Continuidad, se deberá identificar aquellos procesos relacionados a estos productos, y a partir de ellos determinar los procesos críticos para finalmente realizar el análisis de impacto al negocio.

A continuación, se realizará una matriz de doble entrada a efectos de identificar qué procesos están relacionados a los productos de créditos y ahorros; para lo cual

se debe tener en cuenta el catálogo de procesos de la empresa (ver anexo C).

Tabla 10: Procesos relacionados a los productos sobre los cuales se aplicará el SGCN

Procesos de la organización	Productos escogidos para aplicación del SGCN	
	Créditos	Ahorros
Gestión de riesgo crediticio	X	
Gestión de seguridad de la información	X	X
Gestión de continuidad del negocio	X	X
Gestión de producto	X	X
Promoción y venta	X	X
Evaluación	X	
Aprobación	X	
Desembolso	X	
Fondeo por depósitos del público		X
Financiamiento de otras fuentes		X
Venta de servicios	X	X
Afiliación de servicios	X	X
Administración de canales de atención	X	X
Administración de documentos y valorados	X	X
Seguimiento de cartera	X	
Atención al cliente	X	X
Fidelización del cliente	X	X
Gestión de seguros	X	X
Recuperación pre judicial	X	
Recuperación judicial	X	
Refinanciamiento y reprogramados	X	
Castigo y venta de cartera	X	
Administración de tasas y tarifas	X	X

Fuente: Catálogo de procesos de la organización – elaboración propia

Los procesos que se muestran en la tabla son los que se encuentran relacionados a los productos de créditos y ahorros; el universo de procesos se encuentra en el anexo C.

Luego de haber identificado los procesos asociados a los productos de créditos y ahorros, se deberá determinar la criticidad considerando el nivel de impacto en caso de afectación de algunos de estos procesos; para ello se aplicará nuevamente la metodología de impactos (definida en la Norma de Especificación Técnica ISO 22317).

En la siguiente tabla se puede apreciar la identificación de la criticidad de los procesos asociados a los productos de créditos y ahorros.

Tabla 11: Criticidad según proceso asociados a los productos créditos y ahorros

Procesos	IMPACTO					Puntaje
	Financiero	Reputación	Legal y Regulatorio	Contractual	Objetivos de Negocio	
Gestión de producto	2	0	0	5	3	10
Promoción y venta	4	0	0	5	4	13
Evaluación	3	5	5	5	5	23
Aprobación	4	4	5	5	5	23
Desembolso	3	4	5	5	5	22
Fondeo por depósitos del público	5	5	5	5	5	25
Financiamiento de otras fuentes	5	1	0	0	4	10
Venta de servicios	2	2	0	2	2	08
Afiliación de servicios	2	2	3	0	2	09

Procesos	IMPACTO					Puntaje
	Financiero	Reputación	Legal y Regulatorio	Contractual	Objetivos de Negocio	
Administración de canales de atención	0	4	5	3	4	16
Administración de documentos y valorados	0	4	4	3	2	13
Seguimiento de cartera	0	5	0	0	3	08
Atención al cliente	0	2	5	5	4	16
Fidelización del cliente	0	3	0	0	4	07
Gestión de seguros	3	3	5	0	3	14
Recuperación pre judicial	3	3	0	0	4	10
Recuperación judicial	3	3	0	0	4	10
Refinanciamiento y reprogramados	3	2	4	3	2	14
Castigo y venta de cartera	3	2	4	0	3	12
Administración de tasas y tarifas	2	2	4	4	2	14

Fuente: Evaluación realizada por la unidad de continuidad del negocio de la entidad.

4.7.3 Identificación de actividades asociadas a procesos críticos - BIA operativo

Teniendo en cuenta la evaluación realizada, se considerará como críticos a los procesos de: evaluación de clientes, aprobación de créditos, desembolso de

créditos, gestión de canales de atención, atención al cliente, y fondeo por depósito del público.

Luego de haber determinado los procesos críticos, se deberá identificar todas las actividades asociadas a dichos procesos. Para ello es recomendable contar con un diagrama de flujo en el cual se pueda observar la secuencia de las actividades.

Proceso de Evaluación de clientes: El proceso de evaluación consta de tres subprocesos, sub proceso de levantamiento de información, sub proceso de evaluación, y el sub proceso de elaboración de la propuesta de crédito; en el primero se verifica si el cliente cuenta con deudas con atrasos en la entidad, si tiene índices de sobreendeudamiento, así como su calificación en las centrales de riesgo, se visita y se verifica la veracidad del negocio el cual se está evaluando para brindar el crédito, así como las referencias correspondientes; por otra parte, en el subproceso de evaluación, se realiza una evaluación integral del negocio del cliente, la unidad familiar, y las referencias obtenidas en campos, y se procede a elaborar los estados financieros del cliente; finalmente en el tercer sub proceso, relacionado a la elaboración de la propuesta de crédito, consiste en identificar y proponer el crédito más adecuado para el cliente, teniendo en cuenta el plan de inversión presentado, finalmente dichos datos son ingresados al sistema para su posterior aprobación. (ver anexo D)

Proceso de Aprobación de Créditos: En este proceso, se presenta al comité de créditos el expediente del cliente, el cual contiene toda la información recolectada (en el proceso de evaluación) respecto al negocio del cliente, se procede con la verificación de la autenticidad de los documentos presentados, y de ser necesario se solicita la aprobación u opinión de la Gerencia de Riesgos, y finalmente se realiza la aprobación del crédito en el sistema, según el nivel que corresponda. (ver anexo E)

Proceso de Desembolso de Créditos: Previo a realizar el desembolso del crédito, el personal de atención al cliente de las agencias deberá verificar la documentación que se ha recopilado en el expediente, así como informar las condiciones del crédito, tales como el monto aprobado, la fecha de inicio de pago, el importe de la

cuota y el número de cuotas a pagar; luego se procede a solicitar la firma de los clientes y avales en los documentos contractuales, finalmente se genera en ventanilla los documentos correspondientes que aseguren el desembolso del crédito, ya sea en efectivo, a través de abono en cuenta o mediante cheque de gerencia. (ver anexo F)

Proceso de Fondeo Por Depósito del Público: El proceso cuenta con cinco sub procesos: Apertura de cuentas, depósitos, retiros, cancelación de cuentas, y administración y control de cuentas.
En el sub proceso de apertura de cuenta, se solicita al cliente su documento de identificad, se verifica si se encuentra inscrito en el sistema financiero, se procede con la creación de la cuenta de ahorros, y se hace entrega del contrato al cliente. En el sub proceso de retiros, se solicita al cliente su documento de identidad, se validad los datos en el sistema, y se procede con la entrega del efectivo al cliente. (ver anexo G)

Proceso de Gestión de Canales de Atención: A través de este proceso se realizan actividades tales como administración del efectivo en agencia, modificación de datos del cliente, gestión de transacciones (pagos de cuotas, pagos anticipados, pagos adelantados).
En este proceso el ejecutivo de operaciones recibe al cliente en ventanilla, se consulta al cliente que tipo de operación se desea realizar, se efectúa la búsqueda del crédito asociado al cliente en el sistema de créditos, se procede con la impresión del voucher y documentos que correspondan, y finalmente se solicita la firma del cliente en caso de ser necesario. (ver anexo H)

Proceso de Atención al Cliente: Este proceso consiste en atender los requerimientos y reclamos por parte de los clientes de la organización, a través de dos medios, de forma virtual y de forma presencial.
Atención de reclamos de forma virtual: El cliente realiza su reclamo a través de la web de la empresa, posteriormente dicho reclamo es analizado por el Oficial de Atención del Usuario (actualmente Oficial de Conducta de Mercado) y éste emite una respuesta al cliente según el canal que se haya escogido.
Atención de reclamos de forma física: El ejecutivo de servicios recibe al cliente en

la zona de plataforma, se pregunta al cliente qué tipo de consulta desea realizar, se procede con el registro de la solicitud o del reclamo en el sistema web de la empresa, y se entrega un documento en señal de registro del reclamo al cliente, con las indicaciones correspondientes. Posterior a ello, el Oficial de atención al usuario realiza el análisis de la solicitud del cliente y emite una respuesta según el canal que se haya escogido.
(ver anexo I)

Luego de haber identificado las actividades dentro del flujo de cada proceso, se debe determinar los procesos soporte que se encuentran relacionadas a cada actividad, y finalmente identificar adecuadamente los recursos necesarios para el funcionamiento de dichos procesos.

Tabla 12: Resumen de los procesos críticos, sus actividades relacionadas y procesos soporte

PROCESOS	Actividades	Procesos Soporte de las actividades
Evaluación de clientes	Recepción de solicitud de crédito	-
	Evaluación de rechazo en sistema de créditos	Administración de base de datos
	Verificación de DOI en central de riesgo SBS, portales SAT, SUNAT, COFOPRI	Gestión de infraestructura, redes y comunicaciones
		Gestión de riesgo crediticio
	Elabora expediente de visita al cliente	-
	Levantamiento de información – referencias del negocio	-
	Elaboración de 'ficha de unidad familiar'	-
	Evaluación del aval del crédito	Gestión de riesgo crediticio
	Elaboración de EEFF (balance y flujo de ingresos)	Gestión de riesgo crediticio

PROCESOS	Actividades	Procesos Soporte de las actividades
	El ejecutivo de servicios revisa el file del cliente verificando autenticidad de documentación	Gestión de infraestructura, redes y comunicaciones
Aprobación del crédito	Presentar el file de crédito ante el comité de créditos	-
	Exposición de la solicitud ante todos los miembros del comité de créditos	-
	Los integrantes del comité de créditos exponen y describen sus apreciaciones	Gestión de riesgo crediticio
	Si el crédito es mayor a S/. 30 mil, se solicita comentario de la Gerencia de Riesgos	Gestión de riesgo crediticio
	El presidente del comité de créditos evalúa los comentarios y procede con la aprobación del crédito en el sistema.	Gestión de riesgo crediticio
Desembolso del crédito	El ejecutivo de servicios verifica conformidad de documentación del expediente.	Gestión de riesgo crediticio
	Solicita DNI y realiza verificación con RENIEC	Gestión de riesgo crediticio
		Gestión de infraestructura, redes y comunicaciones
	Informa al cliente las condiciones del crédito: importe aprobado, fecha de inicio de pago, importe de cuota, número de cuotas	Gestión de transparencia de información
	Ejecutivo de servicios, verifica importe del crédito y verifica examen médico (crédito superior a S/ 150 mil, y cliente mayor de 40 años)	Gestión de riesgo crediticio

PROCESOS	Actividades	Procesos Soporte de las actividades
	El ESC desbloquea el crédito para desembolso.	-
	El ESC imprime hoja resumen, cronograma de pagos, certificado de seguro de desgravamen, y solicita firma de valorados	Gestión de transparencia de información
	El ESC entrega valorados firmados al cliente.	Gestión de transparencia de información
	a. Desembolso Efectivo	
	El ejecutivo de operaciones (EO) recibe a cliente en ventanilla, solicita y verifica DNI	-
	EO procesa desembolso en sistema, solicita firma y entrega copia de voucher a cliente.	-
	EO entrega efectivo a cliente.	Administración de canales de atención
	b. Desembolso mediante abono en cuenta en la empresa	
	El ESC solicita el llenado del formulario 'sírvase efectuar', con el número de la cuenta para realizar el desembolso del crédito.	Gestión de transparencia de información
	El EO solicita al cliente el DNI y verifica en el sistema.	-
	El EO realiza desembolso en el sistema y emite el voucher al cliente.	Fondeo por depósito del Público
	c. Desembolso mediante cheque de Gerencia o Transferencia	
	El ESC solicita, copia de DNI y el llenado del formulario 'sírvase efectuar',	-

PROCESOS	Actividades	Procesos Soporte de las actividades
	indicando emisión de cheque o transferencia en cuenta.	
	El ESC envía al departamento de tesorería la 'solicitud de crédito', el formato 'sírvase efectuar' y la copia del DNI, y solicita emisión del cheque o transferencia.	Administración de liquidez
	El asistente de tesorería verifica la aprobación del crédito en el sistema	Administración de liquidez
	El asistente de tesorería habilita la cuenta para realizar desembolso mediante cheque o transferencia	Administración de liquidez
	El ESC entrega al EO el formulario 'sírvase efectuar'	-
	El EO, genera el desembolso mediante cheque o transferencia.	-
	El EO genera voucher, solicita firma al cliente y entrega voucher.	-
	El EO emite al área de tesorería el escaneo del voucher.	-
	El asistente de tesorería tramita la emisión del cheque de gerencia o la transferencia correspondiente con la institución financiera.	Administración de liquidez
	El asistente de tesorería comunica la emisión del cheque de Gerencia al Ejecutivo de Servicios.	Administración de liquidez
Fondeo por depósito del Público	**a. Apertura de cuentas**	
	El ESC recibe al cliente y registra sus datos en el sistema	-
	El ESC indica al cliente las condiciones	-

PROCESOS	Actividades	Procesos Soporte de las actividades
	de la apertura y registra en el sistema el tipo de cuenta.	
	El ESC imprime y solicita firma en documentos que correspondan (contrato, cartilla informativa, voucher de apertura)	Gestión de transparencia de información
	El ESC entrega la documentación que corresponda al cliente.	-
	El ESC solicita al cliente realizar el depósito de equilibrio para la apertura correspondiente.	-
	El ESC custodia los documentos hasta su entrega al coordinador de operaciones al cierre del día.	Administración de documentos y valorados
	b.1 Depósito en efectivo	
	El EO solicita al cliente su DNI y el número de cuenta	-
	El EO solicita el efectivo, y procede a realizar el depósito.	-
	El EO genera el voucher, entrega una copia al cliente, y se custodia el original para el cuadre de operaciones al cierre del día.	Administración de documentos y valorados
	b.2 Depósito mediante cheque de gerencia	
	El EO solicita al cliente su DNI, el cheque a depositar, y el número de cuenta destino	-
	El EO registra en el sistema los datos e importe del cheque (en caso el importe supere el umbral permitido, deberá considerarse los filtro	Sistema de prevención de lavado de activos

PROCESOS	Actividades	Procesos Soporte de las actividades
	del sistema PLAFT)	
	El EO imprime voucher, solicita conformidad al cliente, y entrega una copia.	-
	El EO custodia el voucher original, y el cheque en caja buzón hasta el cierre diario.	-
	El coordinador de operaciones (CO) solicita los cheques a los EO y verifica en el sistema la recepción de éstos.	-
	El CO realiza el depósito del cheque en el que tiene cuenta la empresa.	-
	El CO registra en el sistema informático la salida de los cheques, de bóveda a banco.	-
	El CO envía al back office de tesorería la relación de operaciones de depósitos con cheques.	-
	El back office, verifica diariamente en las cuentas, la valorización o rechazo de cheques, y procede con la confirmación en el sistema informático.	-
	El CO verifica la valorización de las operaciones con cheque.	-
	b.3 Depósito mediante transferencia interbancaria	
	El EO solicita al cliente su DNI y copia del voucher de transferencia.	-
	El EO solicita al CO confirmar la transferencia.	-
	El CO solicita al back office la	-

PROCESOS	Actividades	Procesos Soporte de las actividades
	confirmación de la transferencia.	
	El back office verifica que los fondos se encuentren en las cuentas de la institución.	-
	El back office comunica al CO la confirmación de la transferencia.	-
	El EO procede con la ejecución del depósito, imprime el voucher y entrega copia al cliente.	-
	El EO remite al asistente de back office la plantilla de solicitud de valorización de operaciones.	-
	El back office realiza la confirmación de la operación en el sistema informático.	-
	El EO archiva el voucher del depósito.	-
	El CO al finalizar el día realiza el cuadre de operaciones.	Administración de documentos y valorados
	c. Retiro	
	El EO solicita el DNI vigente e identifica en el sistema el número de cuenta.	Administración de base de datos
	El EO valida firma del cliente con firma registrada en el sistema.	-
	El EO registra la operación en el sistema y solicita aprobación del CO.	-
	El CO realiza la autorización correspondiente.	-
	El EO genera la operación, emite el voucher, y solicita firma al cliente.	-
	El EO sella el voucher y entrega copia al cliente.	-
	El EO, entrega efectivo y custodia el	Administración de

PROCESOS	Actividades	Procesos Soporte de las actividades
	voucher original.	documentos y valorados
Gestión de Canales de atención	**a. Pago de cuotas**	
	El EO, recibe al cliente en ventanilla, y solicita documento de identidad.	-
	El EO solicita al cliente el tipo de operación a realizar y procede con su ejecución en el sistema.	-
	El EO, imprime el voucher, entrega una copia al cliente y el original se custodia para el cierre diario.	-
	b. Pago de cuotas (adelantado y anticipado)	
	El EO, recibe al cliente en ventanilla, y solicita documento de identidad.	-
	El EO solicita al cliente el tipo de operación a realizar (pago anticipado, pago adelantado).	-
	El EO entrega el formulario 'sírvase efectuar' al cliente para la confirmación de su elección (pago anticipado, pago adelantado)	Gestión de transparencia de información
	El EO recibe el formulario y registra los datos en el sistema.	Gestión de transparencia de información
	El EO procede con la impresión y la entrega de la copia del voucher al cliente, y el original se custodia para el cierre diario.	-
Atención al Cliente	**a.1 Atención de consultas y requerimientos – presencial**	
	El ESC atiende al usuario en la agencia u oficina especial, y valida su identidad.	-

PROCESOS	Actividades	Procesos Soporte de las actividades
	El ESC registra la solicitud o requerimiento en el aplicativo 'trámite documentario'	Gestión de infraestructura, redes y comunicaciones
	El ESC imprime y gestiona firma de dos formularios, entrega uno al cliente, y custodia otro para la empresa.	-
	El ESC informe al cliente que en un periodo de 30 día se atenderá su requerimiento.	-
	El ESC deriva el requerimiento a la oficina de atención al usuario.	-
	a.2 Atención de consultas y requerimiento – web	
	El analista de atención al usuario recibe el requerimiento o consulta en su correo electrónico.	-
	El analista de atención al usuario analiza el requerimiento o consulta y emite una respuesta vía correo electrónico.	-
	b.1 Atención de reclamos	
	El ESC atiende al usuario en la agencia u oficina especial, y valida su identidad..	-
	El ESC registra el reclamo en el aplicativo 'trámite documentario'	-
	El ESC imprime y gestiona firma de dos formularios, entrega uno al cliente, y custodia otro para la empresa.	-
	El analista de atención al usuario recibe el reclamo y realiza el análisis correspondiente.	-
	El analista de atención al usuario emite	-

PROCESOS	Actividades	Procesos Soporte de las actividades
	el resultado del análisis del reclamo a través de correo.	

Fuente: Normas, manuales y procedimientos de la organización – elaboración propia

4.7.4 Determinación de RTO, RPO, MTPD

Se debe tener en cuenta que en la etapa de análisis de impacto al negocio se busca identificar el grado de afectación que podría tener una empresa debido a algún incidente, el cual ponga en riesgo la continuidad de las operaciones.

Para ello fue necesario identificar los procesos y actividades críticas (obtenidos en el punto 4.7.2 y 4.7.3), los procesos de apoyo, los recursos necesarios para la operatividad de los mismos, tales como software, hardware, personal clave, registros claves, proveedores críticos y similares.

Para este análisis se debe tener en claro las definiciones de RTO, RPO, MTPD.

RTO (*Recovery Time Objetive*): El tiempo objetivo de recuperación se puede entender como el tiempo que tiene una organización para poder reanudar sus operaciones y continuar brindando el producto o servicio afectado.

El RTO se calcula simulando la ejecución de un proceso considerando la ausencia de principales factores tales como, personal clave, sistemas sobre los cuales se soporta las operaciones, proveedores importantes y similares. A efectos de obtener este valor la empresa realizó talleres con los responsables de los procesos con el objetivo de determinar el tiempo que tardarían en reanudar sus procesos ante eventos disruptivos.

RPO (*Recovery Point Objetive*): El punto objetivo de recuperación hace referencia a la cantidad de información que la empresa está dispuesta a perder ante algún incidente que amenace la continuidad de sus operaciones. Para determinar el valor de este parámetro, en los talleres con los dueños de los procesos, se identificó el lugar de almacenamiento de la información que se gestiona en cada proceso, a efectos de determinar la frecuencia con la que se realiza el backup a las bases de

datos y servidores que almacenan dicha información.

MTPD (*Máximum Tolerable Period of Disruption*): El periodo máximo de interrupción tolerable está referido al tiempo máximo que tiene la organización para tener inoperativo sus negocios, antes de que dicha inoperatividad comience a generar pérdidas graves para la empresa, y pongan en riesgo la continuidad de la misma.

Para poder establecer el MTPD, se debe tener en cuenta el apetito al riesgo definido por la empresa. Para establecer dicho apetito, la organización ha considerado tres niveles de impacto cuantificables:

- Impacto en Imagen y Reputación: Considerado como la pérdida de confianza por parte de los clientes o prospecto de clientes, como consecuencia de comentarios negativos y difundidos a través medios de comunicación masivos. Se considera inaceptable tener más de 2000 clientes afectados debido a la inoperatividad de un proceso.
- Impacto legal y de cumplimiento: Suspensión que supere un día de inhabilitación y/o la intervención del regulador. Se considera inaceptable tener multas, sanciones, o suspensiones de actividades que superen las 16 UIT.
- Impacto Financiero: Considerado como pérdidas económicas o ingresos dejados de percibir por un importe que supere los S/. 61 mil.

Considerando lo expuesto se estableció una escala de impactos, que se puede apreciar en la siguiente tabla.

Tabla 13: Nivel de impacto definido para identificación del MTPD

Tipo de Impacto	Nivel de impacto				
	1	2	3	4	5
Imagen y Reputación	Hasta 50 clientes afectados	Hasta 200 clientes afectados	Hasta 500 clientes afectados	Hasta 2000 clientes afectados	Más de 2000 clientes afectados

Tipo de Impacto	Nivel de impacto				
	1	2	3	4	5
Legal y cumplimiento (*)	Hasta 0,5 UIT	Hasta 02 UITs	Hasta 08 UITs	Hasta 16 UITs	Más de 16 UITs
Financiero	S/ 1 mil	S/ 6 mil	S/ 30 mil	S/ 61 mil	Más de S/ 61 mil

Fuente: Información de la Gerencia de Riesgos

(*) Para la presente tabla se consideró una UIT de S/ 3850.

Considerando lo indicado se determinó el RTO, RPO y MTPD de los procesos críticos:

1) Proceso de Evaluación de clientes:

1.1 Determinación de RPO:

Para la etapa de evaluación de créditos, se hace uso del sistema de créditos y del sistema web de RENIEC. Al respecto se confirmó con el departamento de TI que la información que soporta al sistema de créditos se encuentra en una base de datos Oracle, sobre la cual se realiza un proceso de back up diario. Considerando ello el RPO definido para este proceso es de 24 horas.

1.2 Determinación de RTO:

Para determinar el RTO, se identificaron los sistemas que soportan el proceso, y se consultó con el personal de TI los tiempos requeridos para poder reiniciar dichos sistemas y continuar con las operaciones.

Tal como se indicó anteriormente el sistema de créditos, se encuentra soportado en una base de datos Oracle, la cual tiene una réplica en línea. El sistema de créditos (aplicativo cliente servidor), considerando que debe conectarse al servidor de la base de datos réplica ante situaciones de contingencia, tiene un tiempo de configuración y verificación máximo de tres horas y treinta minutos.

Por otra parte, si bien se realizan consultas en el aplicativo web de RENIEC, este

servicio es brindado por el proveedor RENIEC, motivo por el cual no es necesario realizar ninguna configuración, o reinicio del aplicativo. De igual forma sucede con el aplicativo web SBS (portal web de SBS).

Considerando lo expuesto, se establece como RTO para el proceso de evaluación de créditos, un tiempo de 3.5 horas.

1.3 Determinación de MTDP:

Para determinar el MTPD, se considerará, los límites establecidos por el Directorio para cada uno de los tipos de impactos: imagen y reputación, legal y cumplimiento, y financiero.

- Respecto al impacto en imagen y reputación; se identificó con el área de negocios, que la cantidad de clientes atendidos por una agencia u oficina especial, para el proceso de evaluación de créditos, es en promedio 35 clientes diarios. Considerando que se tiene 41 sedes (entre agencias y oficinas especiales), este proceso gestiona un aproximado de 1435 clientes diarios. Finalmente teniendo en cuenta que cada sede opera en el horario de 9:00 am a 6:30 pm (09 horas y 30 minutos), se estimó que en caso este proceso no pueda ejecutarse, se tendrían 151 clientes afectados por hora. Teniendo en cuenta los límites definidos por el Directorio, se aprecia que en 13 horas se llegaría al límite máximo de clientes afectados (2000 clientes). Debido a ello se establece un MTPD para el impacto de imagen y reputación, de 13 horas.
- Respecto al impacto legal y de cumplimiento; el área de negocios en coordinación con el área de operaciones, y el departamento legal, determinaron que el proceso de evaluación de clientes, aprobación y desembolso de créditos deben ser analizados conjuntamente en relación a posibles multas o sanciones que se puedan recibir ante el incumplimiento de estos procesos. Al respecto determinaron que estos procesos en caso no se ejecuten podrían generar multas como consecuencia de protección al consumidor (importe estimado en un tiempo de 24 horas de 50 UIT).
- Respecto al impacto financiero; el área de negocios en coordinación con el área de operaciones, y planeamiento estratégico, determinaron que el proceso de evaluación de clientes, aprobación y desembolso de créditos deben ser analizados conjuntamente con respecto a los ingresos que generan; en razón

dichos ingresos se pueden medir luego que un crédito es efectivamente desembolsado. Al respecto determinaron que estos procesos generan diariamente en promedio ingresos por intereses - de créditos nuevos - por un importe que asciende a S/ 6,8 mil aproximadamente; cabe indicar que para ello las áreas consideraron variables tales como la cantidad de desembolsos diarios realizados, importe promedio de desembolsos, e intereses generados por los desembolsos.

Por otra parte, también se analizó la pérdida que se genera al tener que pagar los salarios de los trabajadores que realizan este proceso, la cual asciende en promedio a S/ 21,1 mil diarios. Considerando estos aspectos, se tiene una pérdida total diaria de S/ 27,9 mil.

Teniendo en cuenta el límite establecido por el Directorio (S/ 61 mil), se aprecia que la organización sólo podría tener inoperativo este proceso aproximadamente por dos días y cuatro horas, antes de empezar a generar pérdidas. Debido a ello se establece un MTPD para el impacto financiero, de 52 horas.

Considerando que el MTPD debe ser el menor tiempo límite identificado en los tres impactos, se establece un MTPD de 13 horas para el proceso de evaluación de créditos.

Tabla 14: MTPD para el proceso de evaluación de clientes

Tipos de Impacto	Tiempo de Inoperatividad								
	1 hr	4hr	8hr	12hr	24hr	2 día	3 días	7 días	MTPD
Imagen y Reputación	2	4	4	4	5	5	5	5	13 hrs
Legal y Cumplimiento	-	-	-	-	5	5	5	5	24 hrs
Financiero	2	2	3	3	3	4	5	5	52 hrs

Fuente: Elaboración propia

Luego de determinar el RTO, el RPO y el MTPD, se identificaron los recursos claves, tales como: personas, instalaciones, equipos, registros clave, y proveedores clave.

1.4 Personal Clave:

- Ejecutivo de Negocios: Responsable de recibir la solicitud de crédito del cliente, realizar la evaluación en centrales de riesgo, verificaciones domiciliarias, y de preparar el file con la documentación que corresponda.
- Ejecutivo de Servicios: En este proceso es responsable de verificar la autenticidad de los documentos del cliente recabados en el file, así como de ingresar dichos datos en el sistema.

1.5 Instalaciones:

Para llevar a cabo el proceso de evaluación de créditos es necesario contar con una oficina, debido a que se requiere tener acceso a la red de la empresa para poder conectarse al sistema de créditos. Se considerará como parte de las instalaciones, la necesidad de tener servicios básicos (energía eléctrica y agua).

1.6 Equipos/recursos:

- Espacio Físico, incluyendo sillas y mesas.
- PC/Laptop, con acceso a internet.
- Impresora

1.7 Registros vitales:

Tabla 15: Detalle de registros vitales – Proceso evaluación de clientes

Registros vitales	Responsable	Custodia
Ficha RENIEC	Ejecutivo de Negocios	Medios físicos
Reporte de nivel de endeudamiento	Ejecutivo de Negocios	Medios físicos
Reporte de Clientes PEP	Ejecutivo de Negocios	Medios físicos
Solicitud de crédito	Ejecutivo de Negocios	Medios físicos
Ficha de ingresos del cliente	Ejecutivo de Negocios	Medios físicos
Ratios financieros y EEFF	Ejecutivo de Negocios	Medios físicos / medios virtuales
Propuesta de crédito	Ejecutivo de Negocios	Medios físicos
Expediente de crédito	Ejecutivo de Negocios	Medios físicos

Fuente: Análisis BIA del proceso de evaluación de clientes - Elaboración propia

1.8 Sistemas de Información/Aplicaciones:

- Windows: Los equipos utilizados por los trabajadores deben contar con el sistema operativo Windows 7 o superior.
- Sistema de créditos: Este aplicativo, debe estar instalado en un servidor Windows Server (mínimamente versión 08), así como en las computadoras de los trabajadores que utilizarán dicho sistema, a fin de poder realizar la evaluación del cliente.
- Navegador web: Se requiere que el navegador web cuente con las extensiones actualizadas, y con el proxy correctamente configurado. Si bien no es indispensable, se recomienda evitar el Internet Explorer y contar con el navegador Chrome o Mozilla Firefox.

1.9 Proveedores Clave:

- RENIEC: Se requiere que el sistema de la RENIEC, se encuentre operativo a efectos de realizar las consultas correspondientes para confirmar la identidad del cliente evaluado.
- SBS: Se requiere que el portal de consulta SBS se encuentre operativo a efectos de poder realizar las consultas referidas a la calificación de riesgo que tiene el cliente.

La interrelación del proceso, con el RPO, RTO, MTPD, instalaciones, equipos/recursos, registros vitales, sistemas de información/aplicaciones, proveedores clave, se puede apreciar en la tabla 15.

Tabla 16: Interrelación de los factores clave en el proceso de evaluación de clientes

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestructura	Servicios
Créditos	Evaluación de Clientes	24 hrs	3.5 hrs	13 hrs	Levantamiento de información	Verificar identidad del cliente	RENIEC	Ejecutivo de Negocios	RENIEC	FICHA RENIEC	- 02 PC - 01 impresora	01 Oficina	Energía Eléctrica / agua
						Verificar al cliente en centrales de riesgo	Internet	Ejecutivo de Negocios	Portal SBS	Reporte de nivel de endeudamiento	- 02 PC - 01 impresora	01 Oficina	Energía Eléctrica / agua
						Verificar si es un cliente PEP	Sistema de Créditos	Ejecutivo de Negocios	-	Reporte de Clientes PEP	- 02 PC - 01 impresora	01 Oficina	Energía Eléctrica / agua
						Registrar solicitud de crédito	Sistema de Créditos	Ejecutivo de Negocios	-	Solicitud de crédito	- 02 PC - 01 impresora	01 Oficina	Energía Eléctrica / agua
						Realizar visita al cliente, y registrar datos de flujo de ingresos	-	Ejecutivo de Negocios	-	Ficha de ingresos del cliente	-	-	-

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestructura	Servicios
					Evaluación de información	Evaluar cualitativa y cuantitativamente al cliente a través de ratios, y EEFF	Sistema de Créditos	Ejecutivo de Negocios	-	Ratios financieros	- 02 PC - 01 impresora	01 Oficina	Energía Eléctrica / agua
					Elaboración de propuesta de crédito	Proponer el producto más adecuado al cliente	Sistema de Créditos	Ejecutivo de Negocios	-	Propuesta de crédito	- 02 PC - 01 impresora	01 Oficina	Energía Eléctrica / agua
						Recopilar la información y trasladar al Ejecutivo de Servicios	-	Ejecutivo de Negocios	-	Expediente de crédito	-	01 Oficina	Energía Eléctrica / agua

Fuente: Análisis BIA del proceso de evaluación de clientes - Elaboración propia

2) Proceso de aprobación de créditos:

2.1 Determinación de RPO:

Para la etapa de aprobación de créditos, se hace uso del sistema de créditos, a través del cual los funcionarios autorizan o deniegan una determinada solicitud. Tal como se ha indicado anteriormente, el sistema de créditos se encuentra en una base de datos Oracle, sobre la cual se realiza un proceso de back up diario. Considerando ello el RPO definido para este proceso es de 24 horas.

2.2 Determinación de RTO:

Para determinar el RTO, se identificaron los sistemas que soportan el proceso, y se consultó con el personal de TI los tiempos requeridos para poder reiniciar dichos sistemas y continuar con las operaciones.

La aprobación de créditos se realiza en el sistema de créditos por los usuarios correspondientes. Como se ha indicado en el proceso de evaluación de créditos, este sistema obtiene la información de una base de datos Oracle, la cual tiene una réplica en línea. Ante situaciones de contingencia, dicho sistema debe estar direccionado a esta base de réplica. Considerando ello el departamento de TI indicó que esta actividad tiene un tiempo de configuración y verificación de tres horas y treinta minutos.

2.3 Determinación de MTDP:

Para determinar el MTPD, se debe tener en cuenta los tipos de impacto: imagen y reputación, legal y cumplimiento, y financiero.

- Respecto al impacto en imagen y reputación; se identificó con el área de negocios, que se tiene siete (07) créditos aprobados en promedio por agencia. Considerando que se cuenta con un total de 41 sedes, este proceso gestiona aproximadamente 287 créditos aprobados por día. Teniendo en cuenta que cada sede opera en el horario de 9:00 am a 6:30 pm (09 horas y 30 minutos), se estimó que en caso este proceso no pueda ejecutarse, se tendrían 30 clientes afectados por hora. Teniendo en cuenta los límites definidos por el Directorio, se aprecia que en 66 horas se llegaría al límite máximo de clientes afectados.
- Respecto al impacto legal y de cumplimiento; el área de negocios en

coordinación con el área de operaciones, y el departamento legal, determinaron que el proceso de evaluación de clientes, aprobación y desembolso de créditos deben ser analizados conjuntamente en relación a posibles multas o sanciones que se puedan recibir ante el incumplimiento de estos procesos. Al respecto determinaron que estos procesos en caso no se ejecuten podrían generar multas como consecuencia de protección al consumidor (importe estimado en un tiempo de 24 horas de 50 UIT).

- Respecto al impacto financiero; tal como se describió para el proceso de evaluación de créditos, se considerará el importe promedio de ingresos generados por intereses de créditos nuevos, el cual asciende aproximadamente a S/ 6,8 mil; más la pérdida que se genera al tener que pagar los salarios de los trabajadores que realizan este proceso, la cual asciende a S/ 27,3 mil. Teniendo en cuenta estos aspectos, se tiene una pérdida total diaria de S/ 34,1 mil.

Considerando el límite establecido por el Directorio (S/ 61 mil), se aprecia que la organización sólo podría tener inoperativo este proceso por 43 horas. Debido a ello se establece un MTPD para el impacto financiero, de 43 horas.

Considerando que el MTPD debe ser el menor tiempo límite identificado en los tres impactos, se establece un MTPD de 24 horas para el proceso de aprobación de créditos.

Tabla 17: MTPD para el proceso de aprobación de créditos

Tipos de Impacto	Tiempo de Inoperatividad								
	1 hr	4hr	8hr	12hr	24hr	2 día	3 días	7 días	MTPD
Imagen y Reputación	1	2	3	3	4	4	5	5	66 hrs
Legal y Cumplimiento	-	-	-	-	5	5	5	5	24 hrs
Financiero	2	2	3	3	4	5	5	5	43 hrs

Fuente: Elaboración propia

Luego de determinar el RTO, el RPO y el MTPD, se identificaron los recursos claves, tales como: personas, instalaciones, equipos, registros clave, proveedores

clave.

2.4 Personal Clave:

- Ejecutivos de Negocios: Responsables de participar en el análisis del crédito propuesto.
- Gerente de Agencia / Ejecutivo de Negocios Senior: Responsable de aprobar los créditos propuestos por los ejecutivos de negocios.
- Gerente de Negocios: Nivel superior para aprobación de créditos que superen un determinado importe.
- Gerente de Riesgos: Nivel superior para aprobación de créditos que presenten excepciones, tales como clientes mal calificados en centrales de riesgos, clientes que superan el ratio de capacidad de pago, u otros motivos.

2.5 Instalaciones:

Para llevar a cabo el proceso de aprobación de créditos es necesario contar con una oficina, debido a que se requiere tener acceso a la red de la empresa para poder registrar las aprobaciones en el sistema de créditos. Se considerará como parte de las instalaciones, la necesidad de tener servicios básicos (energía eléctrica y agua).

2.6 Equipos/recursos:

- Espacio Físico, incluyendo sillas y mesas.
- PC/Laptop, con acceso a internet.

2.7 Registros vitales:

Tabla 18: Detalle de registros vitales – Proceso aprobación de créditos

Registros vitales	Responsable	Custodia
Expediente de Crédito	El ejecutivo de negocios.	Medios físicos
Solicitud de crédito aprobada	Gerente de Agencia / EDN Senior / Gerente Riesgos / Gerente de Negocios	Medios Físicos / virtual

Fuente: Análisis BIA del proceso de aprobación de créditos - Elaboración propia

2.8 Sistemas de Información/Aplicaciones:

- Windows: Los equipos utilizados por los trabajadores deben contar con el sistema operativo Windows 7 o superior.
- Sistema de créditos: Este aplicativo, debe estar instalado en las computadoras, a fin de poder realizar la aprobación del crédito.

2.9 Proveedores Clave:

No se tienen proveedores clave en este proceso

La interrelación del proceso, con el RPO, RTO, MTPD, instalaciones, equipos/recursos, registros vitales, sistemas de información/aplicaciones, proveedores clave, se puede apreciar en la tabla 18.

Tabla 19: Interrelación de los factores clave en el proceso de aprobación de créditos

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestructura	Servicios
Créditos	Aprobación de créditos	24 hrs	3.5 hrs	24 hrs	Aprobación de créditos	Revisión del crédito propuesto	-	Gerente de Agencia / Ejecutivo de negocios Senior	-	Aprobación en Expediente de Crédito	-	01 Oficina	Energía Eléctrica / agua
						Levantamiento de observaciones	Sistema de Créditos	Gerente de Negocios / Gerente de Riesgos	-	Reporte de observaciones superadas	01 PC	01 Oficina	Energía Eléctrica / agua
						Aprobación en sistema	Sistema de Créditos	Gerente de Agencia / Ejecutivo de negocios Senior	-	Aprobación en el sistema	01 PC	01 Oficina	Energía Eléctrica / agua

Fuente: Análisis BIA del proceso de aprobación de créditos - Elaboración propia

3) Proceso de desembolso de créditos:

3.1 Determinación de RPO:

Para esta etapa, se hace uso del sistema de créditos, a través del cual los ejecutivos de operaciones realizan el desembolso de los créditos, a través de sus diferentes modalidades, en efectivo, transferencia o cheque. Al respecto se confirmó con el departamento de TI que la información que soporta al sistema de créditos se encuentra en una base de datos Oracle, sobre la cual se realiza un proceso de back up diario. Considerando ello el RPO definido para este proceso es de 24 horas.

3.2 Determinación de RTO:

Para determinar el RTO, se identificaron los sistemas que soportan el proceso, y se consultó con el personal de TI los tiempos requeridos para poder reiniciar dichos sistemas y continuar con las operaciones.

El desembolso se realiza en el sistema de créditos, por el personal de caja (ejecutivos de operaciones), como ya se indicó, este sistema obtiene información de una base de datos Oracle, la cual tiene una réplica en línea. Ante situaciones de contingencia, dicho sistema debe estar direccionado a esta base de réplica. Considerando ello el departamento de TI indicó que esta actividad tiene un tiempo de configuración y verificación de tres horas y treinta minutos.

3.3 Determinación de MTDP:

Para determinar el MTPD, se debe tener en cuenta los tipos de impacto: imagen y reputación, legal y cumplimiento, y financiero.

- Respecto al impacto en imagen y reputación; se identificó con el área de negocios, que se tiene en promedio 211 créditos desembolsados por día. Teniendo en cuenta que cada sede opera en el horario de 9:00 am a 6:30 pm (09 horas y 30 minutos), se estimó que en caso este proceso no pueda ejecutarse, se tendrían 22 clientes afectados por hora. Teniendo en cuenta los límites definidos por el Directorio, se aprecia que en 90 horas (aproximadamente 04 días) se llegaría al límite máximo de clientes afectados.
- Respecto al impacto legal y de cumplimiento; el área de negocios en coordinación con el área de operaciones, y el departamento legal, determinaron

que el proceso de evaluación de clientes, aprobación y desembolso de créditos deben ser analizados conjuntamente en relación a posibles multas o sanciones que se puedan recibir ante el incumplimiento de estos procesos. Al respecto determinaron que estos procesos en caso no se ejecuten podrían generar multas como consecuencia de protección al consumidor (importe estimado en un tiempo de 24 horas de 50 UIT).

- Respecto al impacto financiero; tal como se describió para el proceso de evaluación de créditos, se considerará el importe promedio de ingresos generados por intereses de créditos nuevos, el cual asciende aproximadamente a S/ 6,8 mil; más la pérdida que se genera al tener que pagar los salarios a los trabajadores que realizan este proceso, la cual asciende a S/ 4,7 mil. Teniendo en cuenta estos aspectos, se tiene una pérdida total diaria de S/ 11,5 mil.

Considerando el límite establecido por el Directorio (S/ 61 mil), se aprecia que la organización sólo podría tener inoperativo este proceso por 127 horas (aproximadamente 05 días). Debido a ello se establece un MTPD para el impacto financiero, de 05 días.

Considerando que el MTPD debe ser el menor tiempo límite identificado en los tres impactos, se establece un MTPD de 24 horas para el proceso de desembolso de créditos.

Tabla 20: MTPD para el proceso de aprobación de desembolso de créditos

Tipos de Impacto	Tiempo de Inoperatividad								
	1 hr	4hr	8hr	12hr	24hr	2 día	3 días	7 días	MTPD
Imagen y Reputación	1	2	2	3	4	4	4	5	04 días
Legal y Cumplimiento	-	-	-	-	5	5	5	5	24 hrs
Financiero	1	2	2	2	3	3	4	5	05 días

Fuente: Elaboración propia

Luego de determinar el RTO, el RPO y el MTPD, se identificaron los recursos claves, tales como: personas, instalaciones, equipos, registros clave, proveedores

clave.

3.4 Personal Clave:

- Ejecutivos de Operaciones: Responsables de verificar la veracidad de la documentación y de realizar el desembolso.
- Ejecutivo de servicios: Responsable de recopilar la documentación necesaria del cliente para realizar el desembolso.
- Coordinador de operaciones: Responsable de aprobar los desembolsos en determinados casos (cuando se supera un determinado límite); así como para habilitar efectivo a los ejecutivos de operaciones.

3.5 Instalaciones:

Para llevar a cabo el proceso de desembolso de créditos es necesario contar con una oficina, debido a que se requiere tener acceso a la red de la empresa para poder realizar las transacciones en el sistema de créditos. Se considerará como parte de las instalaciones, la necesidad de tener servicios básicos (energía eléctrica y agua).

3.6 Equipos/recursos:

- Espacio Físico, incluyendo sillas y mesas.
- PC/Laptop, con acceso a internet.
- Impresoras, y ticketera.

3.7 Registros vitales:

Tabla 21: Detalle de registros vitales – Proceso desembolso de créditos

Registros vitales	Responsable	Custodia
Expediente de Crédito	Ejecutivo de negocios	Medios físicos
Contrato	Ejecutivo de servicios	Medios físicos
Hoja Resumen	Ejecutivo de servicios	Medios físicos
Certificado de Desgravamen	Ejecutivo de servicios	Medios físicos
Voucher de desembolso	Ejecutivo de Operaciones	Medios físicos

Fuente: Análisis BIA del proceso de desembolso de créditos - Elaboración propia

3.8 Sistemas de Información/Aplicaciones:

- Windows: Los equipos utilizados por los trabajadores deben contar con el sistema operativo Windows 7 o superior.
- Sistema de créditos: Este aplicativo, debe estar instalado en un servidor Windows Server (mínimamente versión 08), así como en las computadoras de los trabajadores que utilizarán dicho sistema, a fin de poder realizar la evaluación del cliente.
- Navegador web: Se requiere que el navegador web cuente con las extensiones actualizadas, y con el proxy correctamente configurado. Si bien no es indispensable, se recomienda evitar el Internet Explorer y contar con el navegador Chrome o Mozilla Firefox.

3.9 Proveedores Clave:

RENIEC: Para confirmar la identidad del cliente se requiere realizar consultas a la página web de RENIEC.

La interrelación del proceso, con el RPO, RTO, MTPD, instalaciones, equipos/recursos, registros vitales, sistemas de información/aplicaciones, proveedores clave, se puede apreciar en la tabla 21.

Tabla 22: interrelación de los factores clave en el proceso de desembolso de créditos

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestructura	Servicios
Créditos	Desembolso de Créditos	24 hrs	3.5 hrs	24 hrs	Contacto y firmas del cliente	Verificar conformidad de documentación de expedientes	Internet	Ejecutivo de Servicios	RENIEC	Expediente	03 PC	01 Oficina	Energía Eléctrica / agua
						Desbloquear el crédito en el sistema	Sistema de créditos	Ejecutivo de Servicios	-	-	03 PC	01 Oficina	Energía Eléctrica / agua
						Impresión y firma de valorados	Sistema de Créditos	Ejecutivo de Servicios	-	- Contrato - Hoja Resumen - Cronograma - Certif. Desgravamen	- 03 PC - 01 impresora	01 Oficina	Energía Eléctrica / agua
					Generación del desembol	Verificación de identidad	Internet	Ejecutivo de Operacio	RENIEC	-	03 PC	01 Oficina	Energía Eléctrica / agua

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestructura	Servicios
					so			nes					
						Procesa desembolso y emite voucher	Sistema de Créditos	Ejecutivo de Operaciones	-	voucher	- 03 PC - 03 Ticketera	01 Oficina	Energía Eléctrica / agua

Fuente: Análisis BIA del proceso de desembolso de créditos - Elaboración propia

4) Fondeo por depósito del Público:

4.1 Determinación de RPO:

El proceso de fondeo por depósito del público hace uso de un aplicativo web (TOPAZ) el cual utiliza información de una base de datos Oracle. Esta base de datos se encuentra en el mismo servidor que la base de datos del sistema de créditos. El departamento de TI, indicó que para esta base de datos también se realiza un backup diario. Considerando ello se establece un RPO de 24 horas para este proceso.

4.2 Determinación de RTO:

Para determinar el RTO, se identificaron los sistemas que soportan el proceso, y se consultó con el personal de TI los tiempos requeridos para poder reiniciar dichos sistemas y continuar con las operaciones.

Tal como se indicó anteriormente el sistema de pasivos (TOPAZ) el cual es utilizado para realizar la captación de los fondos del público, es un aplicativo web que obtiene información de una base de datos Oracle, la cual cuenta con una réplica en línea.

Ante situaciones de contingencia o caídas de la base de datos principal, el aplicativo de pasivos debe conectarse al servidor alterno. El departamento de TI ha evidenciado que esta actividad tiene un tiempo de configuración de cuatros horas; esto debido a que debe redirigir enlaces, y realizar pruebas de funcionamiento.

Por otra parte, si bien se realizan consultas en el aplicativo web de RENIEC, este servicio es brindado por el proveedor RENIEC, motivo por el cual no es necesario realizar ninguna configuración, o reinicio del aplicativo.

Considerando ello, se establece como RTO para el proceso de fondeo por depósitos del público, un tiempo de cuatro horas.

4.3 Determinación de MTDP:

Para determinar el MTPD, se considerará, los límites establecidos por el Directorio para cada uno de los tipos de impacto: imagen y reputación, legal y cumplimiento, y financiero. El análisis se realizará para cada uno de los sub procesos:

Tabla 23: Identificación del MTPD del proceso de fondeo por depósito al público

Tipo de Impacto:	**Imagen y Reputación**
Resultado MTPD – Impacto en imagen y reputación: 08 horas y 30 minutos	
Apertura de Cuentas	Este sub proceso atiende en promedio 05 clientes por agencia. Considerando que se tiene 41 sedes, se gestiona un aproximado de 205 clientes diarios. Finalmente teniendo en cuenta que cada sede opera en el horario de 9:00 am a 6:30 pm (09 horas y 30 minutos), se estimó que en caso este proceso no pueda ejecutarse, se tendrían 22 clientes afectados por hora. Teniendo en cuenta los límites definidos por el Directorio, se aprecia que en 90 horas se llegaría al límite máximo de clientes afectados (2000 clientes).
Depósitos	Se ha estimado que a través de este sub proceso se atienden diariamente en promedio a 55 clientes por agencia, que representan a 2255 clientes a nivel nacional. Esto representa a 238 clientes por hora, debido a ello se llegaría al límite máximo de clientes afectados en 8.5 horas.
Retiros	Se ha estimado que este sub proceso gestiona aproximadamente 18 clientes en promedio por agencia, haciendo un total de 738 clientes a nivel nacional. Esto representa a 78 clientes por hora, debido a ello se llegaría al límite máximo de clientes afectados en 26 horas.
Cancelación de Cuentas	Se ha estimado que este sub proceso gestiona aproximadamente 03 clientes en promedio por agencia, haciendo un total de 123 clientes a nivel nacional. Esto representa a 13 clientes por hora, debido a ellos se llegaría al límite máximo de clientes afectados en 154 horas.
Administración y Control de Cuentas	Para este sub proceso no aplica realizar una estimación, en razón que está referido a la gestión de la cartera de pasivos; y no existe relación directa con el cliente.
Tipo de Impacto:	**Legal y de Cumplimiento**
Resultado MTPD – Impacto legal y de cumplimiento: 09 horas y 30 minutos	
Apertura de Cuentas	Para este sub proceso no aplica ningún impacto legal en razón que se tiene a prospectos de clientes con quienes no se tiene ninguna relación contractual.

Depósitos	Para este sub proceso no aplica ningún impacto legal en razón que no existen multas por no aceptar el depósito de un cliente ante situaciones de contingencia.
Retiros	Para este sub proceso no aplica ningún impacto legal.
Cancelación de Cuentas	Para este sub proceso se asume que un cliente no puede realizar la cancelación de su cuenta de ahorros, lo que implica un incumplimiento al Reglamento de Conducta de Mercado; aspecto que puede conllevar a una multa de hasta 50 UIT. Se considera para este sub proceso que no se brindó servicios durante todo un día (09 horas y 30 minutos). Por ello se considera un MTPD de 09 horas y 30 minutos.
Administración y Control de Cuentas	Este sub proceso gestiona la cartera de pasivos, y tiene entre sus principales actividades, el cálculo de intereses. Al respecto se pudo apreciar que en caso no se paguen los intereses de los clientes, puede conllevar a una multa de hasta 100 UIT. El cálculo de intereses se realiza de forma diaria; debido a ello se establece un MTPD de 24 horas, en razón que posterior a las 24 horas de no realizar el cálculo de los intereses podría conllevar a la multa indicada.
Tipo de Impacto:	**Financiero**
Resultado MTPD – Impacto financiero: 05 horas	
Apertura de Cuentas	Se determinó que este sub proceso gestiona un ingreso aproximado de S/ 125 mil diarios; asimismo se considera una pérdida por salarios por S/ 1,5 mil; teniendo en cuenta estos aspectos se tiene una pérdida total de S/ 126,5 mil. Considerando el límite establecido por el Directorio (S/ 61 mil), se aprecia que la organización solo podría tener inoperativo este proceso durante 05 horas.
Depósitos	Se determinó que este sub proceso gestiona un ingreso aproximado de S/ 26 mil diarios; asimismo se considera una pérdida por salarios por S/ 1,4 mil; teniendo en cuenta estos aspectos se tiene una pérdida total de S/ 27,4 mil. Considerando el límite establecido por el Directorio (61 mil), se aprecia que la organización solo podría tener inoperativo este proceso

	durante 21 horas.
Retiros	Asumiendo que no se pueda ejecutar este sub proceso, no genera impacto financiero.
Cancelación de Cuentas	Asumiendo que no se pueda ejecutar este sub proceso, no genera impacto financiero. Sí genera impacto regulatorio, el cual fue analizado previamente.
Administración y Control de Cuentas	Asumiendo que no se pueda ejecutar este sub proceso, no genera impacto financiero.

Fuente: Información de la Gerencia de Riesgos

Considerando que el MTPD debe ser el menor tiempo límite identificado en los tres impactos, se establece un MTPD de 05 horas para el proceso de evaluación de créditos.

Tabla 24: MTPD para el proceso de fondeo por depósitos del público

Tipos de Impacto	Tiempo de Inoperatividad								
	1 hr	4hr	8hr	12hr	24hr	2 día	3 días	7 días	MTPD
Imagen y Reputación	3	4	4	5	5	5	5	5	8.5 hrs
Legal y Cumplimiento	-	-	-	5	5	5	5	5	9.5 hrs
Financiero	3	4	5	5	5	5	5	5	05 hrs

Fuente: Elaboración propia

Luego de determinar el RTO, el RPO y el MTPD, se identificaron los recursos claves, tales como: personas, instalaciones, equipos, registros clave, proveedores clave.

4.4 Personal Clave:

- Ejecutivo de Servicios: Responsable de brindar la información al cliente respecto a los beneficios y riesgos del producto, para posteriormente recibir las solicitudes de apertura de cuentas pasivas, y recopilar la documentación

correspondiente.

- Ejecutivo de Operaciones: En este proceso es responsable de verificar la autenticidad de los documentos del cliente recabados en el file, y proceder con la apertura de la cuenta en el sistema de pasivos.
- Coordinador de Operaciones: Responsable de realizar habilitaciones del terminal financiero hacia bóveda en caso se supere el límite de efectivo.

4.5 Instalaciones:

Para llevar a cabo el proceso de fondeo por depósito del público es necesario contar con una oficina, debido a que se requiere tener acceso a la red de la empresa para poder conectarse al sistema de pasivos. Se considerará como parte de las instalaciones, la necesidad de tener servicios básicos (energía eléctrica y agua).

4.6 Equipos/recursos:

- Espacio Físico, incluyendo sillas y mesas.
- PC/Laptop, con acceso a internet.
- Impresora

4.7 Registros vitales:

Tabla 25: Detalle de registros vitales – Proceso de fondeo por depósito al público

Registros vitales	Responsable	Custodia
Formato de Solicitud de apertura de cuenta	Ejecutivo de servicios.	Medios físicos
Copia de DNI del cliente	Ejecutivo de servicios	Medios Físicos
Contrato	Ejecutivo de servicios	Medios Físicos
Cartilla Informativa	Ejecutivo de servicios	Medios Físicos
Carta de traslado (en el caso de CTS)	Ejecutivo de servicios	Medios Físicos
Voucher	Ejecutivo de operaciones	Medios Físicos

Fuente: Análisis BIA del proceso de fondeo por depósito al público - Elaboración propia

4.8 Sistemas de Información/Aplicaciones:

- Windows: Los equipos utilizados por los trabajadores deben contar con el sistema operativo Windows 7 o superior.

- Sistema de pasivos: Este aplicativo, debe estar instalado en las computadoras, a fin de poder realizar la apertura de las cuentas.
- Navegador web: Se requiere que el navegador web cuente con las extensiones actualizadas, y con el proxy correctamente configurado. Si bien no es indispensable, se recomienda evitar el Internet Explorer y contar con el navegador Chrome o Mozilla Firefox.

4.9 Proveedores Clave:

- TOPCOR: Proveedor que brinda soporte al aplicativo de pasivos (TOPAZ) ante alguna situación de contingencia.
- RENIEC: Para confirmar la identidad del cliente se requiere realizar consultas a la página web de RENIEC.

La interrelación del proceso, con el RPO, RTO, MTPD, instalaciones, equipos/recursos, registros vitales, sistemas de información/aplicaciones, proveedores clave, se puede apreciar en la tabla 25.

Tabla 26: Interrelación de los factores clave en el proceso de fondeo por depósito del público

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestructura	Servicios
Ahorros	Fondeo por depósito del público	24 hrs	04 hrs	05 hrs	Apertura de cuentas	Registro de datos de cliente	Sistema de Pasivos	Ejecutivo de Servicios	- TOPCORP - RENIEC	- Formato de solicitud de apertura	02 PC	01 Oficina	Energía Eléctrica / agua
						Impresión y firma de documentos	Sistema de Pasivos	Ejecutivo de Servicios	TOPCORP	- Contrato - Cartilla Informativa - Copia de DNI - Carta de traslado de CTS (para CTS)	- 02 PC - 01 Impresora	01 Oficina	Energía Eléctrica / agua
						Depósito para apertura	Sistema de Pasivos	Ejecutivo de Operaciones	TOPCORP	Voucher de depósito	- 02 PC - 02 ticketera	01 Oficina	Energía Eléctrica / agua
					Depósitos	Solicita DNI, y registra el importe a depositar	Sistema de Pasivos	Ejecutivo de Operaciones	TOPCORP	-	01 PC	01 Oficina	Energía Eléctrica / agua
						Imprime y entrega el	Sistema de Pasivos	Ejecutivo de Operaciones	TOPCORP	Voucher de depósito	- 02 PC - 02	01 Oficina	Energía Eléctrica /

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestructura	Servicios
						voucher					ticketera		agua
					Retiros	Verifica identidad del cliente	Sistema de Pasivos	Ejecutivo de Operaciones	- TOPCORP - RENIEC	-	01 PC	01 Oficina	Energía Eléctrica / agua
						Registra operación	Sistema de Pasivos	Ejecutivo de Operaciones	TOPCORP	-	01 PC	01 Oficina	Energía Eléctrica / agua
						Aprobación del retiro	Sistema de Pasivos	Coordinador de Operaciones	TOPCORP	-	01 PC	01 Oficina	Energía Eléctrica / agua
						Genera retiro y emite voucher	Sistema de Pasivos	Ejecutivo de Operaciones	TOPCORP	Voucher de retiro (firmado)	- 01 PC - 01 ticketera	01 Oficina	Energía Eléctrica / agua
					Cancela-ción de cuentas	Verifica identidad del cliente	Sistema de Pasivos	Ejecutivo de Operaciones	- TOPCORP - RENIEC	-	01 PC	01 Oficina	Energía Eléctrica / agua
						Registra la operación	Sistema de Pasivos	Ejecutivo de Operaciones	TOPCORP	-	01 PC	01 Oficina	Energía Eléctrica / agua
						Aprobación de la cancelación	Sistema de Pasivos	Coordinador de Operaciones	TOPCORP	-	01 PC	01 Oficina	Energía Eléctrica / agua

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestructura	Servicios
						Imprime voucher de cancelación y solicita firmas	Sistema de Pasivos	Ejecutivo de Operaciones	TOPCORP	Voucher firmado por el cliente	- 01 PC - 01 ticketera	01 Oficina	Energía Eléctrica / agua
					Adminis-tración y control de cuentas	Proceso diario contable	Sistema de Pasivos y Sistema de Créditos	Operador de TI	-	Reporte de confirmación de procesos correcto	01 PC	01 Oficina	Energía Eléctrica / agua
						Impresión diaria de reporte de cancelaciones	Sistema de Pasivos	Coordinador de Operaciones	TOPCORP	Reporte de cancelaciones	01 PC	01 Oficina	Energía Eléctrica / agua

Fuente: Análisis BIA del proceso de fondeo por depósito al público - Elaboración propia

5) Gestión de Canales de Atención:

5.1 Determinación del RPO:

Este proceso tiene actividades relacionadas a la atención del cliente; tales como la gestión de pagos de cuotas de un crédito (considerando los pagos adelantados y pagos anticipados). Estos pagos son registrados en el sistema de créditos, el cual, como se ha visto anteriormente tiene un RPO definido de 24 horas.

5.2 Determinación de RTO:

Para determinar el RTO, se identificaron los sistemas que soportan el proceso, y se consultó con el personal de TI los tiempos requeridos para poder reiniciar dichos sistemas y continuar con las operaciones.

Las transacciones relacionadas a pago de cuotas se realizan en el sistema de créditos, el cual, tal como se ha indicado anteriormente obtiene información de una base de datos Oracle, que tiene una réplica en línea. Ante situaciones de contingencia, dicho sistema debe estar direccionado a esta base de réplica. Considerando ello el departamento de TI indicó que esta actividad tiene un tiempo de configuración y verificación de tres horas y treinta minutos.

5.3 Determinación del MTPD:

Para determinar el MTPD, se debe tener en cuenta los tipos de impacto: imagen y reputación, legal y cumplimiento, y financiero.

- Respecto al impacto en imagen y reputación; se identificó con el área de negocios, que se tiene en promedio 235 clientes atendidos en este proceso por día. Teniendo en cuenta que cada sede opera en el horario de 9:00 am a 6:30 pm (09 horas y 30 minutos), se estimó que en caso este proceso no pueda ejecutarse, se tendrían 25 clientes afectados por hora. Teniendo en cuenta los límites definidos por el Directorio, se aprecia que en 80 horas (aproximadamente 3.5 días) se llegaría al límite máximo de clientes afectados. Debido a ello se establece un MTPD para el impacto de imagen y reputación, de 80 horas.
- Respecto al impacto legal y de cumplimiento; en caso este proceso no se encuentre operativo, podría ocasionar no registrar los pagos de los clientes de

forma oportuna, aspecto que podría generar que se reporte con calificación incorrecta al cliente en la central de riesgos. Lo descrito podría conllevar a una multa de hasta 50 UIT. Para que un cliente sea reportado incorrectamente, tendría que considerarse atraso en su pago, mínimo de un día, debido a ello se considera un MTPD para el impacto legal y de cumplimiento, de 24 horas.

- Respecto al impacto financiero; se debe tener en cuenta que en caso este proceso no se ejecute, no genera un impacto financiero directo en la organización; cabe indicar que los impactos por multas o sanciones fueron considerados en el punto anterior.

Considerando que el MTPD debe ser el menor tiempo límite identificado en los tres impactos, se establece un MTPD de 24 horas para el proceso de gestión de canales de atención.

Tabla 27: MTPD para el proceso de gestión de canales de atención

Tipos de Impacto	Tiempo de Inoperatividad								
	1 hr	4hr	8hr	12hr	24hr	2 día	3 días	7 días	MTPD
Imagen y Reputación	1	2	2	3	4	4	4	5	80 hrs
Legal y Cumplimiento	-	-	-	-	5	5	5	5	24 hrs
Financiero	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Fuente: Elaboración propia

Luego de determinar el RTO, el RPO y el MTPD, se identificaron los recursos claves, tales como: personas, instalaciones, equipos, registros clave, proveedores clave.

5.4 Personal Clave:

- Ejecutivo de Operaciones: Responsable de recibir el efectivo por parte del cliente, y realizar los registros correspondientes a las cancelaciones de cuotas en el sistema de créditos.

5.5 Instalaciones:

Para llevar a cabo el proceso de fondeo por depósito del público es necesario contar con una oficina, debido a que se requiere tener acceso a la red de la empresa para poder conectarse al sistema de pasivos. Se considerará como parte de las instalaciones, la necesidad de tener servicios básicos (energía eléctrica y agua).

5.6 Equipos/recursos:

- Espacio Físico, incluyendo sillas y mesas.
- PC/Laptop, con acceso a internet.
- Ticketera

5.7 Registros vitales:

Tabla 28: Detalle de registros vitales – Proceso de gestión de canales de atención

Registros vitales	Responsable	Custodia
Voucher	Ejecutivo de Operaciones	Medios físicos
Formato sírvase efectuar	Ejecutivo de Operaciones	Medios físicos
Nuevo cronograma (para pagos anticipados)	Ejecutivo de Operaciones	Medios físicos
Reporte de flujos diarios	Ejecutivo de Operaciones	Medios físicos
Formato de remesas	Ejecutivo de Operaciones	Medios físicos

Fuente: Análisis BIA del proceso de gestión de canales de atención - Elaboración propia

5.8 Sistemas de Información/Aplicaciones:

- Sistema de créditos: Este aplicativo, debe estar instalado en las computadoras, a fin de poder realizar el registro de la cancelación de cuotas.
- Windows: Los equipos utilizados por los trabajadores deben contar con el sistema operativo Windows 7 o superior.
- Navegador web: Se requiere que el navegador web cuente con las extensiones actualizadas, y con el proxy correctamente configurado. Si bien no es indispensable, se recomienda evitar el Internet Explorer y contar con el navegador Chrome o Mozilla Firefox.

5.9 Proveedores Clave:

- PROSEGUR: Proveedor que brinda servicios de traslado de valorados.

La interrelación del proceso, con el RPO, RTO, MTPD, instalaciones, equipos/recursos, registros vitales, sistemas de información/aplicaciones, proveedores clave, se puede apreciar en la tabla 28.

Tabla 29: Interrelación de los factores clave en el proceso de gestión de canales de atención

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestruc.	Servicios
Créditos / Ahorros	Gestión de canales de atención	24 hrs	3.5 hrs	24 hrs	Administración del efectivo	Revisión diaria del saldo de efectivo en bóveda	Sistema de créditos	Coordinador de Operaciones / Ejecutivo de Operaciones	-	Reporte de flujos diarios	01 PC	01 Oficina	Energía Eléctrica / agua
						Solicitud de remesas	Sistema de créditos	Coordinador de operaciones	PROSEGUR	Formato de remesas	-	01 Oficina	Energía Eléctrica / agua
					Administración del personal de atención al cliente (ventanilla)	Coordinar la gestión de accesos para ejecutivos y coordinadores de operaciones	Sistema de créditos	Analista de Help Desk	-	-	01 PC	01 Oficina	Energía Eléctrica / agua
					Gestión de transacciones	Gestiona el tipo de pago (normal, anticipado,	Sistema de créditos	Ejecutivo de Operaciones	-	Formato de pago adelantado/ anticipado	01 PC	01 Oficina	Energía Eléctrica / agua

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestruc.	Servicios
						adelantado)							
						Registro del pago	Sistema de créditos	Ejecutivo de Operaciones	-	-	01 PC	01 Oficina	Energía Eléctrica / agua
						Emisión del voucher	Sistema de créditos	Ejecutivo de Operaciones	-	Voucher	01 PC	01 Oficina	Energía Eléctrica / agua

Fuente: Análisis BIA del proceso de proceso gestión de canales de atención - Elaboración propia

6) Atención al Cliente

6.1 Determinación del RPO:

Este proceso gestiona las solicitudes y reclamos efectuados por el cliente. Estos reclamos se realizan a través de una plataforma web, la cual deposita su información en una base de datos SQL, y sobre la cual se realiza un procedimiento de backup diario. Considerando ello, se establece como RPO 24 horas.

6.2 Determinación de RTO:

Para determinar el RTO, se consultó con el personal de TI el tiempo que requieren para poder restaurar el servicio web de consultas y reclamos.

Tal como se indicó en el punto anterior, este servicio web deposita su información en una base de datos SQL, sobre la cual se realiza un proceso de backup diario; al respecto el departamento de TI indicó que en caso de pérdida de información el tiempo estimado para poder realizar una restauración de la base de datos desde la cinta de respaldo es de tres horas. Teniendo en cuenta ello se establece un RTO de 03 horas.

6.3 Determinación del MTPD:

Para determinar el MTPD, se debe tener en cuenta los tipos de impacto: imagen y reputación, legal y cumplimiento, y financiero.

- Respecto al impacto en imagen y reputación; en coordinación con el área de operaciones, y el Oficial de Atención al Usuario (OAU) se identificó que se registran aproximadamente 3 reclamos cada hora a nivel de todas las agencias. Teniendo en cuenta los límites definidos por el Directorio, se aprecia que en 27 días se llegaría al límite máximo de clientes afectados (2000 clientes). Debido a ello se establece un MTPD para el impacto de imagen y reputación, de 27 días.
- Respecto al impacto legal y de cumplimiento; en caso este proceso no se encuentre operativo durante un día, podría conllevar a una multa de hasta 150 UIT, debido a ello se considera un MTPD para el impacto legal y de cumplimiento, de 24 horas.
- Respecto al impacto financiero; se debe tener en cuenta que en caso este proceso no se ejecute, no genera un impacto financiero directo en la

organización; cabe indicar que los impactos por multas o sanciones fueron considerados en el punto anterior.

Considerando que el MTPD debe ser el menor tiempo límite identificado en los tres impactos, se establece un MTPD de 24 horas para el proceso de atención al cliente.

Tabla 30: MTPD para el proceso de atención al cliente

Tipos de Impacto	Tiempo de Inoperatividad								
	1 hr	4hr	8hr	12hr	24hr	2 día	3 días	7 días	MTPD
Imagen y Reputación	1	1	1	1	2	2	3	4	27 días
Legal y Cumplimiento	-	-	-	-	5	5	5	5	24 hrs
Financiero	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Fuente: Elaboración propia

Luego de determinar el RTO, el RPO y el MTPD, se identificaron los recursos claves, tales como: personas, instalaciones, equipos, registros clave, proveedores clave.

6.4 Personal Clave:

- Ejecutivo de Servicios: Responsable de recibir al cliente en las instalaciones de la organización y realizar el registro del reclamo en la plataforma web.
- Oficial de Atención al Usuario: Responsable de analizar la solicitud y/o reclamo del cliente y emitir una respuesta dentro de los tiempos establecidos.

6.5 Instalaciones:

Si bien los requerimientos y reclamos se pueden realizar en las instalaciones de las agencias; es posible prescindir de dichas instalaciones para este proceso, en razón que este servicio se encuentra habilitado vía web para uso de los clientes.

6.6 Equipos/recursos:

- Espacio Físico, incluyendo sillas y mesas.
- PC/Laptop, con acceso a internet.
- Impresora

6.7 Registros vitales:

Tabla 31: Detalle de registros vitales – Proceso de atención al cliente

Registros vitales	Responsable	Custodia
Formato de requerimiento/reclamo	Oficial de Atención al Usuario	Medios físico y virtuales
Respuesta a requerimiento/reclamo	Oficial de Atención al Usuario	Medios físico y virtuales

Fuente: Análisis BIA del proceso de atención al cliente - Elaboración propia

6.8 Sistemas de Información/Aplicaciones:

- Servicio web de reclamos: No es necesario contar con el ningún aplicativo instalado, para acceder a este servicio se requiere de acceso a internet.
- Windows: Los equipos utilizados por los trabajadores deben contar con el sistema operativo Windows 7 o superior.
- Navegador web: Se requiere que el navegador web cuente con las extensiones actualizadas, y con el proxy correctamente configurado. Si bien no es indispensable, se recomienda evitar el Internet Explorer y contar con el navegador Chrome o Mozilla Firefox.

6.9 Proveedores Clave:

Se cuenta con un consultor encargado de realizar las modificaciones a los códigos fuente de la página web.

La interrelación del proceso, con el RPO, RTO, MTPD, instalaciones, equipos/recursos, registros vitales, sistemas de información/aplicaciones, proveedores clave, se puede apreciar en la tabla 31.

Tabla 32: Interrelación de los factores clave en el proceso de atención al cliente

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestructura	Servicios
Ahorros	Fondeo por depósito del público	24 hrs	04 hrs	05 hrs	Atención de consultas	Registro de la consulta en aplicativo web	Web de reclamos	Ejecutivo de Servicios	-	Formato de solicitud de información	- 01 PC - Impresora	01 Oficina	Energía Eléctrica / agua
						Análisis de la solicitud por parte del analista	Web de reclamos	Analista	-	Formato de solicitud de información	01 PC	01 Oficina	Energía Eléctrica / agua
						Respuesta al cliente	Correo	Analista	-	Correo de respuesta	01 PC	01 Oficina	Energía Eléctrica / agua
					Atención de reclamos	Registro del reclamo en aplicativo web	Web de reclamos	Ejecutivo de Servicios	-	Formato de reclamos	- 01 PC - Impresora	01 Oficina	Energía Eléctrica / agua
						Análisis del reclamo	Web de reclamos	Oficial de Atención al Usuario	-	Formato de reclamos	01 PC	01 Oficina	Energía Eléctrica / agua
						Respuesta al	Correo	Oficial	-	Correo de	01 PC	01 Oficina	Energía

Producto / Servicio	Proceso Crítico	RPO	RTO	MTPD	Sub Proceso	Actividades	Aplicaciones / Sistemas informáticos	Personal clave	Proveedores clave	Registros clave	Equipos	Infraestructura	Servicios
						cliente		de Atención al Usuario		respuesta			Eléctrica / agua

Fuente: Análisis BIA del proceso de proceso de atención al cliente - Elaboración propia

4.8 Gestión de riesgos

La gestión integral de riesgos es considerada hoy en día como un aspecto primordial del Gobierno Corporativo en muchas empresas. Tal es el caso que la SBS estableció para su aplicación desde el 2018, el Reglamento de Buen Gobierno Corporativo y de la Gestión Integral de Riesgos.

La gestión integral de riesgos, incluye en su tipología a los riesgos operacionales, dentro de los cuales se encuentran enmarcados los riesgos de continuidad del negocio.

Se debe tener en cuenta que toda organización, independientemente del tamaño, estructura o naturaleza, se encuentra expuesta a riesgos. Considerando lo indicado, el objetivo principal de esta etapa, consiste en identificar los diversos escenarios que pudieran afectar o poner en peligro la continuidad de los productos o servicios que brinda la organización.

Para ello se debe tener en cuenta conceptos fundamentales, tales como riesgo, riesgo inherente, riesgo residual, probabilidad e impacto.

Riesgo:

- En el Marco Integrado de Control Interno – COSO, se entiende como riesgo a la posibilidad de que ocurra un determinado evento y éste afecte de forma negativa a la consecución de los objetivos de la organización.[14]
- El Reglamento de Gobierno Corporativo y de Gestión Integral de Riesgos, define al riesgo como '*Posibilidad de ocurrencia sobre los objetivos de la empresa o su situación financiera*'.[15]
- Por otra parte, la Guía ISO-CEI 73:2009, define al riesgo como '*la combinación de la probabilidad de un suceso y de su consecuencia*'[16]

Riesgo Inherente y riesgo residual:

- El Marco Integrado de Control Interno – COSO, describe al riesgo inherente como aquel que repercute negativamente en la consecución de los objetivos de la

[14] Everson et al. (2013). Control Interno – Marco Integrado.
[15] Resolución SBS Nª 272-2017. Diario Oficial del Bicentenario El Peruano. Lima, Perú, 18 de enero del 2017.
[16] ISO Guía 73:2009, definición 2.1

organización sin haber adoptado medidas que alteren la probabilidad o impacto del riesgo.

- Por otro lado, se describe al riesgo residual, como aquel que afecta al cumplimiento de los objetivos, y que permanece aún después de haberse adoptado e implementado controles que mitiguen los riesgos inherentes.

La relación entre el riesgo inherente y residual se puede representar considerando la siguiente fórmula:

Riesgo Inherente – Controles = Riesgo Residual

Probabilidad:

- La Guía ISO-CEI 73:2009, define este aspecto como el grado en que ocurre un determinado evento.

Impacto:

- La Guía ISO-CEI 73:2009, define este aspecto como el resultado de un determinado evento.

Control:

- El Reglamento de Gobierno Corporativo y de Gestión Integral de Riesgos, define como control a aquel *proceso que busca asegurar que las medidas de respuesta al riesgo se cumplan de acuerdo con lo previsto*.
- Finalmente, la Guía ISO-CEI 73:2009, determina que el control hace referencia a las *acciones que ponen en aplicación las decisiones de la gestión de riesgos*.

En ese sentido, se consideraron los siguientes aspectos para la evaluación de riesgos y controles de la gestión de continuidad del negocio:

- Identificación de las principales amenazas que pudieran impactar significativamente las operaciones de la organización.
- Identificar los principales componentes que soportan los procesos de la organización, los cuales en caso de ser afectados pudieran generar un evento de

riesgo que impacte en la continuidad del negocio.

- Identificar controles que permitan mitigar los posibles eventos de riesgo.
- Identificar y evaluar los eventos de riesgo.
- Recomendar mejoras a los actuales controles y/o proponer nuevos controles que permitan mitigar los riesgos identificados.

4.8.1 Identificación de amenazas

Como se ha mencionado anteriormente, toda organización se encuentra expuesta a potenciales riesgos. Sin embargo, en diversas investigaciones se suele asociar erróneamente la continuidad del negocio sólo con eventos relacionados a desastres naturales, sin considerar que existen múltiples amenazas que también ponen en riesgo la continuidad operativa de los distintos servicios de una organización.

En el reporte anual de nombre '*Horizon Scan Report 2017*' emitido por el Business Continuity Institute (BCI) se describen las principales amenazas, según encuestas realizadas a 726 organizaciones distribuidas en 79 países, obteniendo el siguiente resultado:

1. Ataques cibernéticos
2. Violación de datos
3. Interrupciones de TI y telecomunicaciones
4. Incidentes de seguridad
5. Cambios climatológicos
6. Interrupción de servicios básicos
7. Actos de terrorismo
8. Interrupción de la cadena de suministro
9. Disponibilidad de habilidades clave
10. Nuevas leyes y cambios en la regulación

Por otra parte, es importante señalar las tendencias que podrían ocasionar un futuro impacto en la gestión de continuidad. En el reporte mencionado anteriormente se indica que estas tendencias son: la influencia de las redes sociales, constantes cambios políticos, cambios constantes en la mentalidad y necesidades del cliente, y

bajo crecimiento económico y su impacto en la inversión.

Considerando lo descrito anteriormente, se realizaron diversos talleres a efectos de identificar las amenazas y riesgos que afecten a la organización, obteniendo entre los principales riesgos a los siguientes:

Tabla 33: Principales riesgos de la organización

Proceso afectado	Riesgo	Amenaza
• Todos los procesos	Daños en la infraestructura física de la oficina principal y/o agencias de la organización.	Incendios / Terremotos / Inundaciones
• Todos los procesos	Daños en el Centro de Procesamiento de Datos (equipos de comunicaciones, servidores, ambientes de desarrollo, calidad y producción).	Incendios / Terremotos
• Todos los procesos	Indisponibilidad de los servicios de TI (servicio de base de datos, correo, sistema de créditos, sistema de ahorros).	Incendios / Terremotos / Ciberataques
• Todos los procesos	Inaccesibilidad de los trabajadores y clientes a las instalaciones de la organización.	Incendios / Terremotos / Inundaciones / Huelgas
• Desembolso de Crédito • Fondeo por depósitos del público • Gestión de canales de atención	Ausencia de efectivo en las agencias para atención al cliente.	Incendios / Terremotos / Robos
• Desembolso de Crédito • Fondeo por depósitos del público	Posibles multas y/o sanciones debido a pérdida de registros vitales tales como contratos de créditos y ahorros, hojas resumen, cartillas informativas, certificados de desgravamen.	Incendios / Terremotos / Inundaciones / Personal no apto

• Todos los procesos	Posibles multas y/o sanciones debido a incumplimientos de nuevas normas o modificaciones en la regulación que conlleven al cierre de una agencia	Nuevas normas / Cambios en la regulación

Fuente: Talleres de evaluación de riesgos - Elaboración propia

4.8.2 Identificación de componentes de afectación

Para efectos de la presente tesis, se considera un componente de afectación al elemento que soporta los procesos de la organización, y cuya indisponibilidad afectaría de modo determinante la continuidad de los mismos. Así tenemos:

- Personas: Se evalúa la indisponibilidad del personal involucrado en la ejecución de los procesos de la empresa.
- Infraestructura: Se evalúa la indisponibilidad de las instalaciones o ambientes físicos (incluyendo servicios básicos de electricidad, agua, desagüe, etc.).
- Recursos: Se evalúa la indisponibilidad de mobiliario, insumos y/o equipos necesarios para la operación (escritorios, sillas, PCs, impresoras, teléfonos, etc.).
- Registros vitales: Se evalúa la indisponibilidad de recursos relacionados a información y/o documentación clave, para la realización de las operaciones.
- Sistemas de información: Se evalúa la indisponibilidad o falla de los aplicativos o sistemas informáticos que soportan los procesos de negocio y/o apoyo de la organización.
- Proveedores críticos: Se evalúa la indisponibilidad de los principales proveedores que soportan los procesos de la organización.

Teniendo en cuenta cada uno de los riesgos identificados, se relacionaron los componentes que pudieran ser afectados en caso se materialicen dichos riesgos.
Se debe tener en cuenta que, para el análisis de riesgo, se debe considerar el mayor impacto y probabilidad obtenido según el componente afectado.

Tabla 34: Ejemplo de evaluación de riesgos

Riesgo:	Indisponibilidad de los servicios de TI

Componentes:	Personas	Infraestructura	Recursos	Registros Vitales	Sistemas de Información	Proveedores Críticos
Marque con x los componentes afectados				x	x	
Determinación de probabilidad e impacto por componente						
Probabilidad				Posible	Improbable	
Impacto				Relevante	Moderado	
Nivel de riesgo					Moderado	Bajo
Determinación de probabilidad e impacto final						
Probabilidad	Posible					
Impacto	Relevante					
Nivel de Criticidad	Moderado					

Fuente: Metodología de identificación y evaluación de riesgos de la organización

4.8.3 Identificación de Controles

Previamente a realizar la evaluación de riesgos, se deberá identificar los controles existentes y analizar el nivel de efectividad que tienen éstos respecto a los componentes de afectación.

Tabla 35: Ejemplo de aplicación de controles en riesgos

Riesgo:		Indisponibilidad de los servicios de TI						Efectividad	Reduce P/I
Componentes:		Personas	Infraestructura	Recursos	Registros Vitales	Sistemas de Información	Proveedores Críticos		
Marque con x los componentes afectados					x	x	x		
C001	Cláusula de continuidad de negocio en los contratos con proveedores						x	PE	P
C002	Evaluaciones de seguridad por externos					x		E	P
C008	Firewalls					x		E	P
C020	Antivirus				x	x		E	I
C021	IPS				x	x		PE	I
C030	Campañas de seguridad de información				x	x		E	P
C001	Proxys				x	x		E	P
C001	VPN SSL				x	x		E	P
C001	Sistemas de Respaldos (Bakcups)				x	x		E	P/I
Determinación de probabilidad e impacto por componente								Efectividad	Reduce

								P/I
Probabilidad				Posible	Improbable		E	P
Impacto				Relevante	Moderado			
Nivel de riesgo				Moderado	Bajo			
Determinación de probabilidad e impacto final								
Probabilidad	Posible							
Impacto	Relevante							
Nivel de Criticidad	Moderado							

Fuente: Metodología de identificación y evaluación de riesgos de la empresa caso de estudio

Se debe analizar el nivel de efectividad que tiene cada uno de los controles, respecto a los riesgos identificados, a efectos de determinar si estos en su conjunto reducen el nivel de impacto o probabilidad, para ello se deben considerar las características del control.

- Formalizado y/o documentado: Identificar si el control se encuentra formalizado (descrito en alguna norma) y genera evidencia.
- Periodicidad de ejecución: Identificar la frecuencia con la que se ejecuta el control, de forma diaria, mensual, trimestral, semestral y/o anual.
- Periodicidad de pruebas: Identificar con qué frecuencia se realizan pruebas para probar el control.
- Tipo de control: Identificar el tipo de control, preventivo, detectivo, correctivo
- Reduce Impacto o Probabilidad: Indicar qué atributo de riesgo disminuye la ejecución del control.
- Nivel de Automatización: Identificar si el control que se realiza es manual, semi automático, o automático.
- Responsable: Identificar el responsable de la ejecución del control.

Tabla 36: Ejemplo de aplicación de tributos de medición de la efectividad del control

Código	Descripción del control	Detalle del Control							
		Formalizado y/o documentado	Periodicidad de ejecución	Periodicidad del mantenimiento/ pruebas	Tipo de Control	Reduce Probabilidad o impacto	Automatización	Responsable	Nivel de efectividad resultante
C001	Cláusula de continuidad de negocio en los contratos con proveedores	SI	N/A	N/A		P	M		PE
C002	Evaluaciones de seguridad por externos	SI	T	A		P	SA		E
C008	Firewalls	SI	N/A	A		P	SA		E
C020	Antivirus	SI	N/A	A		I	SA		E
C021	IPS	SI	N/A	A		I	SA		PE

C030	Campañas de seguridad de información	SI	M	S		P	M		E
C001	Proxys	NO	N/A	A		P	SA		E
C001	VPN SSL	SI	M	A		P	SA		E
C001	Sistemas de Respaldos (Bakcups)	SI	D	S		P	SA		E

Fuente: Metodología de identificación y evaluación de riesgos de la empresa caso de estudio

4.8.4 Evaluación de Riesgos

Para estimar el nivel de exposición de los riesgos de continuidad, se realizó una evaluación de la probabilidad y el impacto que tendrían los riesgos identificados en caso de materializarse.

Se debe tener en cuenta que el nivel de riesgo para cada amenaza se calcula considerando el mayor nivel de riesgo resultante de todos los componentes afectados.

Para esta evaluación se consideró una matriz de cinco por cinco (05 niveles de probabilidad y 05 niveles de impacto), y cuatro niveles de criticidad:

a. **Probabilidad**:

Tabla 37: Parámetros de probabilidad

Nro.	Probabilidad	Descripción
1	Raro	El evento se presenta cada 05 años o más
10	Improbable	El evento se presenta cada 03 años
50	Posible	El evento se presenta cada año
75	Probable	El evento se presenta cada 06 meses
100	Casi certeza	El evento se presenta cada mes

Fuente: Manual de gestión de riesgos de la organización

b. **Impacto**:

Tabla 38: Parámetros de impacto

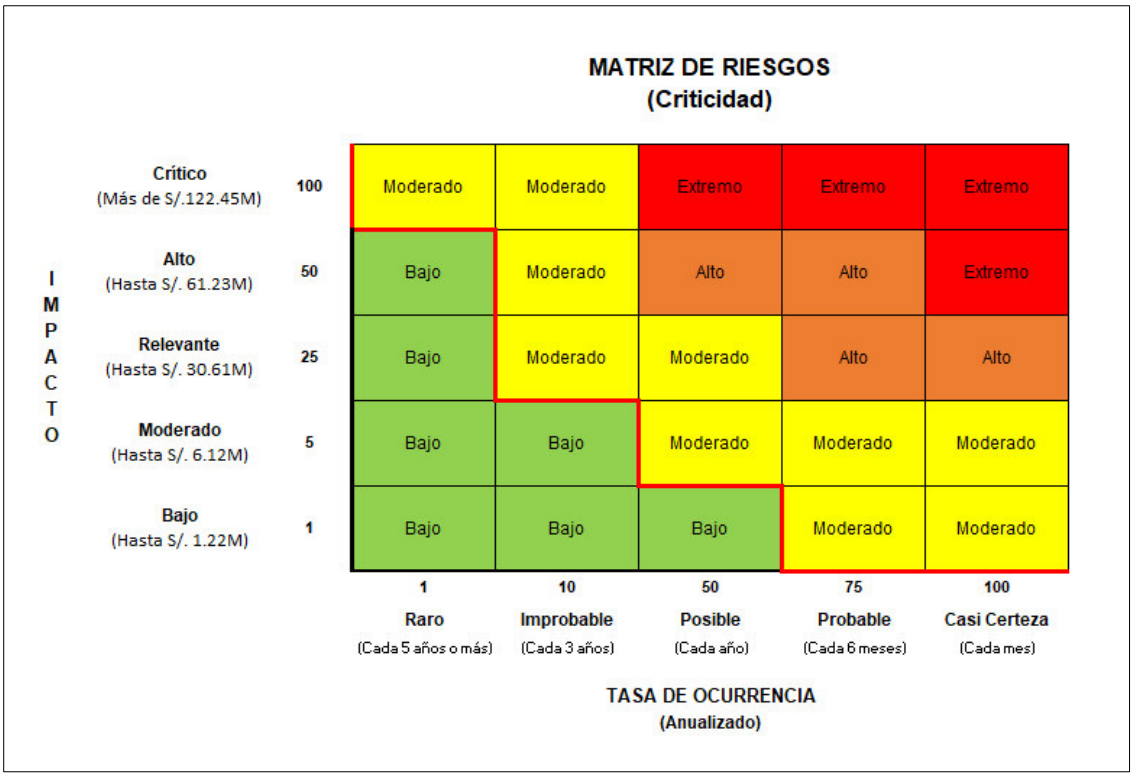
Nro.	Impacto	Tipo	Descripción

1	Bajo	Financiera	Pérdida financiera de hasta S/ 1,22 mil
		Disponibilidad	El efecto es nulo o muy pequeño en la operación de la sede
5	Moderado	Financiera	Pérdida financiera superior a S/ 1,22 mil hasta S/ 6,12 mil
		Disponibilidad	El evento puede afectar hasta 04 horas la operación de la sede
25	Relevante	Financiera	Pérdida financiera superior a S/ 6,12 mil hasta S/ 30,61 mil
		Disponibilidad	El evento puede afectar entre 04 horas y 01 día la operación de la sede
50	Alto	Financiera	Pérdida financiera superior a S/ 30,61 mil hasta S/ 61,23 mil
		Disponibilidad	El evento puede afectar entre 02 y 04 días la operación de la sede
100	Crítico	Financiera	Pérdida financiera superior a S/ 61,23 mil
		Disponibilidad	El evento puede afectar entre una o más semanas la operación de la sede

Fuente: Manual de gestión de riesgos de la organización

c. **Nivel de Riesgo**: Para la determinación del nivel de riesgo criticidad, se debe tener en cuenta la combinación de los valores de probabilidad e impacto:

Figura 8: Mapa de calor de Riesgos



Fuente: Matriz de riesgos de la empresa caso de estudio - Confidencial

En donde:

Tabla 39: Descripción del nivel de criticidad

Criticidad	Requiere Tratamiento	Plazo de Implementación	Rango (miles)	Descripción
Extremo	SI	03 meses	< 4,592 - 12,245]	Riesgo no deseable, que requiere acción correctiva inmediata, dentro del apetito y tolerancia al riesgo (03 meses)
Alto	SI	06 meses	<1,531 - 4,592]	Riesgo no deseable, que requiere acción correctiva, dentro del apetito y tolerancia al riesgo (06 meses)
Moderado	SI	09 meses	<61 – 1,153]	Riesgo no deseable, que requiere acción correctiva no inmediata, dentro del apetito y tolerancia al riesgo (09 meses)

Criticidad	Requiere Tratamiento	Plazo de Implementación	Rango (miles)	Descripción
Bajo	NO	No Aplica	[0 – 61]	Riesgo aceptable sin revisión.

Fuente: Manual de gestión de riesgos de la organización

Considerando lo expuesto se puede apreciar que se debe brindar tratamiento a los riesgos que tengan un nivel de criticidad, moderado, alto, y extremo.

4.8.5 Tratamiento de los riesgos de Continuidad

Tal como se mencionó anteriormente, luego de determinar el nivel de criticidad de los riesgos identificados, se debe realizar tratamiento a aquellos que tienen un nivel riesgo de moderado, alto y extremo. Para ello se identificaron los controles existentes, y se analizó la posibilidad de realizar mejoras o implementar nuevos controles, que permitan incrementar el nivel de efectividad a fin de reducir el nivel de riesgo obtenido en la evaluación. Este aspecto es evaluado en la etapa de selección de estrategias.

La empresa definió los siguientes niveles de riesgo para su medición:

Tabla 40: Nivel de criticidad residual de los riesgos de continuidad identificados

Proceso	ID	Riesgo	Escenario	Causa	Probabilidad		Impacto		Nivel de Riesgo Inherente	Controles	Nivel de Riesgo Residual
					Descripción	Valor	Descripción	Valor			
	RCN - 001	Daños en la infraestructura física de la oficina principal y/o agencias de la organización.	Terremoto	Cambios climatológicos constantes	Raro	1	Crítico	100	Moderado	Establecer señalización, rutas de escape, puertas de emergencia, y puntos de encuentro en caso de desastre. Establecer brigadas de emergencia. Programar y ejecutar simulacros de forma periódica. Establecer contratos de seguros contra todo riesgo.	Moderado
			Incendios	Acciones generadas por personas / Cortocircuitos	Posible	50	Crítico	100	Extremo	Implementar sistema de alarmas contra incendios, sensores de humo.	Alto

Proceso	ID	Riesgo	Escenario	Causa	Probabilidad		Impacto		Nivel de	Controles	Nivel de
										Distribuir extintores en puntos críticos.	
										Establecer brigadas de emergencia.	
										Establecer contratos de seguros contra todo riesgo.	
	RCN - 002	Daños en el centro de procesamiento de datos (CPD) (equipos de comunicaciones, servidores, ambientes de desarrollo, calidad y producción).	Incendios	Acciones generadas por personas / Cortocircuitos	Posible	50	Crítico	100	Extremo	Implementar sistema de alarmas contra incendios, sensores de humo.	Alto
										Distribuir extintores en puntos críticos (Tipo C)	
										Establecer brigadas de emergencia.	
										Implementar un centro de procesamiento de datos alterno.	
										Desarrollar y ejecutar procedimientos de backup para los servidores con información crítica.	

Proceso	ID	Riesgo	Escenario	Causa	Probabilidad		Impacto		Nivel de	Controles	Nivel de
										Establecer contratos de seguros contra todo riesgo.	
			Inundaciones	Fallas en los servicios de agua que generen aniego	Posible	50	Crítico	100	Extremo	Implementar piso falso/ elevado en todo el ambiente. Implementar un centro de procesamiento de datos alterno. Establecer contratos de seguros contra todo riesgo.	Alto
	RCN - 003	Indisponibilidad de los servicios de TI (servicio de base de datos, correo, sistema de créditos, sistema de ahorros).	Ciberataques	Continuos ataques informáticos que deterioran o ponen en riesgo los servicios brindados por la organización	Casi Certeza	100	Alto	50	Extremo	Implementar un software para detectar malware (antivirus) con alcance a todo el parque informático. Configurar correctamente el firewall Configurar correctamente el proxy Instalar herramientas	Alto

Proceso	ID	Riesgo	Escenario	Causa	Probabilidad		Impacto		Nivel de	Controles	Nivel de
										contra spam, phishing.	
										Realizar copias de seguridad sobre la información crítica de la organización.	
										Establecer una política de gestión de accesos que considere perfiles según el puesto del trabajador, contraseñas robustas, etc.	
										Establecer procedimientos manuales para: atención de reclamos, evaluación de clientes, aprobación de créditos, desembolso de créditos, apertura de cuentas, cobro de cuotas, y retiro de efectivo de cuentas.	

Proceso	ID	Riesgo	Escenario	Causa	Probabilidad		Impacto		Nivel de	Controles	Nivel de
			Indisponibilidad del Proveedor	Ausencia de servicios principales, agua y electricidad	Casi Certeza	100	Relevante	25	Alto	Implementar grupos electrógenos	Moderado
	RCN - 004	Inaccesibilidad de los trabajadores y clientes a las instalaciones de la organización.	Huelgas / Problemas sociales	Huelgas que ponen riesgo la integridad de las personas y clientes, forzando a cerrar las instalaciones.	Posible	50	Alto	50	Alto	Establecer planes de comunicaciones (comunicados en página web) Establecer brigadas de emergencia. Establecer alianzas estratégicas con cajeros corresponsales y el Banco de la Nación para poder realizar la atención del proceso de créditos.	Moderado
	RCN - 005	Ausencia de efectivo en las agencias para	Indisponibilidad del Proveedor	Indisponibilidad del proveedor para atender las	Casi Certeza	100	Relevante	25	Alto	Arqueo diario por parte del Coordinador de Operaciones a efectos	Moderado

Proceso	ID	Riesgo	Escenario	Causa	Probabilidad		Impacto		Nivel de	Controles	Nivel de
		atención al cliente.		remesas solicitadas por la agencia con déficit de efectivo						de identificar los flujos de efectivo. Establecer acuerdos de niveles de servicio (SLA)	
	RCN - 006	Posibles multas y/o sanciones debido a pérdida de registros vitales tales como contratos de créditos y ahorros, hojas resumen, cartillas informativas, certificados de desgravamen.	Incendio	Acciones generadas por personas / Cortocircuitos	Posible	50	Crítico	100	Extremo	Implementar sistema de alarmas contra incendios, sensores de humo. Distribuir extintores en puntos críticos. Establecer brigadas de emergencia. Realizar copias de seguridad sobre la información crítica de la organización. Establecer contratos de seguros contra todo riesgo.	Alto
			Inundaciones	Fallas en los servicios de agua que generen aniego	Posible	50	Crítico	100	Extremo	Establecer contratos de seguros contra todo riesgo.	Alto

Proceso	ID	Riesgo	Escenario	Causa	Probabilidad		Impacto		Nivel de	Controles	Nivel de
			Errores del personal	Ausencia de personal con el conocimiento y habilidades necesarias para el desarrollo de esta actividad	Casi Certeza	100	Relevante	25	Alto	Implementar evaluaciones técnicas en los procesos de reclutamiento Programas de capacitación periódicos según las funciones de cada puesto de trabajo. Establecer procedimientos disciplinarios y las medidas a adoptar en casos de faltas recurrentes.	Moderado
	RCN - 007	Posibles multas y/o sanciones debido a incumplimientos de nuevas normas o modificaciones en la regulación que conlleven al cierre de una agencia	Errores del personal	No identificar constantemente la nueva regulación aplicable a la organización	Casi Certeza	100	Moderado	5	Moderado	Identificar periódicamente la nueva regulación aplicable a la organización. Establecer comités de cumplimiento normativo en el cual se expongan las nuevas normas y el estado de	Bajo

Proceso	ID	Riesgo	Escenario	Causa	Probabilidad		Impacto		Nivel de	Controles	Nivel de
										los planes de acción a adoptar por la organización.	

Fuente: Evaluación de riesgos realizada por la empresa

4.9 Evaluación y selección de estrategias

Posterior a realizar la identificación y análisis de riesgos, se deben determinar las estrategias más adecuadas que permitan mitigar dichos riesgos.

El objetivo de esta etapa, es seleccionar las medidas necesarias que permitan a la organización protegerse y contar con las soluciones para la recuperación de las funciones críticas de la empresa.

Las estrategias, dependiendo de la organización suelen ir desde las más exigentes, conocidas también como 'zonas calientes' hasta alternativas simples denominadas como 'zonas frías'.

Tabla 41: Tipos de estrategias

Estrategia	Descripción
Sitio Caliente	Esta estrategia supone la existencia de un sitio alterno, que cuente con replicación de la operación primaria. En estas instalaciones se debe contar con todas las aplicaciones instaladas, servidores operando adecuadamente, y estaciones de trabajo listas.
Traslado a otros centros del grupo	Esta estrategia consiste en contar con un sitio alterno ubicado en un ambiente físico que pertenece a la organización, pero fuera de la sede principal que realiza las operaciones. Este tipo de estrategias generalmente es utilizado por grandes organizaciones que cuentan con diversas instalaciones. El sitio alterno se encuentra disponible y en espera para ser utilizado ante la ocurrencia del evento disruptivo.
Trabajo a Distancia	Este tipo de estrategias suele utilizarse para determinadas actividades del proceso. Se considera dentro de estas estrategias, todos los trabajos que se realicen fueran de los ambientes físicos de la empresa,
Sitio tibio	Esta estrategia considera ambientes con equipos, recursos y enlaces configurados de forma parcial. La capacidad del CPU es menor a la de producción normal.
Acuerdo recíproco	Estrategia en la cual se debe contar con acuerdos definidos con otras

Estrategia	Descripción
	empresas, de forma que ante algún incidente la organización pueda trasladar sus operaciones. Para elegir este tipo de estrategias, se considera que la empresa receptora debe tener infraestructura tecnológica similar y compatible con la empresa que sufre el evento disruptivo.
Sitio móvil	Esta estrategia está orientada principalmente a contar con un ambiente físico 'móvil' (como es el caso de containers), que puedan transportarse de forma rápida a un lugar alterno. Para este tipo de ambientes, suele contarse con equipos configurados, servidores, computadoras y enlaces.
Sitio frío	Esta estrategia implica contar con un lugar que tenga instalaciones eléctricas, y ventilación. Se considera que el lugar se encuentra disponible para la recepción del equipo en casos de emergencia; sin embargo no se cuenta con hardware de computación.
Recuperación y restauración	Este tipo de estrategia se basa principalmente en la contratación de seguros. No se cuentan con sitios alternos de operación. Se considera que este tipo de estrategias es adecuado para organizaciones con un apetito de riesgo moderado o sitios de baja criticidad.
Ninguna estrategia	Al elegir esta opción se debe considerar que no se tendrá documentación de recuperación y continuidad del negocio. Este aspecto se presenta generalmente en organizaciones con alto nivel de apetito por el riesgo o de un sitio con baja criticidad.

Fuente: Cooperación económica y Técnica (2013). La continuidad de negocios y operaciones frente a situaciones de desastre en América Latina y el Caribe. Balance y recomendaciones.

Tabla 42: Ventajas y desventajas de las estrategias

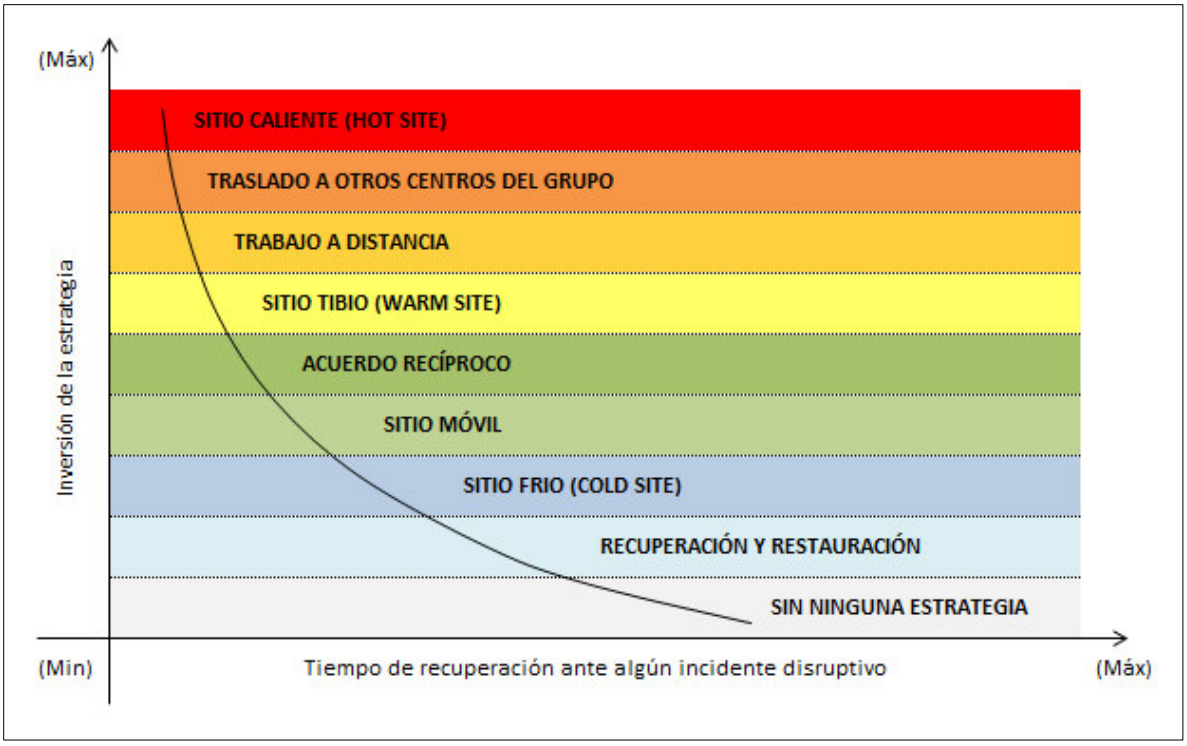
Estrategia	Ventajas	Desventajas
Sitio Caliente	Disponibilidad de los ambientes 24/7, los cuales tienen exclusividad de uso.	Alto costo, debido a que requiere de constante mantenimiento de hardware, software, aplicaciones y

Estrategia	Ventajas	Desventajas
		datos; además de los niveles de seguridad que deben establecerse.
Traslado a otros centros del grupo	Existe una rápida respuesta de activación frente a cualquier evento; más aun considerando que las instalaciones deben contar con la misma tecnología con la que se opera en la sede principal.	Costo elevado.
Trabajo a Distancia	Se considera que estas estrategias son flexibles y orientas sobre todo a entidades pequeñas.	Podría haber fuga de información debido a débiles controles de seguridad y confidencialidad.
Sitio tibio	Menos costoso que contar con un sitio caliente.	Se podría sobre valorar las capacidades de procesamiento.
Acuerdo recíproco	Se estima que corresponde a estrategias fáciles de implementar, en razón que la tecnología utilizada por la empresa receptora es similar a la de la empresa que presenta el evento disruptivo.	Dificultad para encontrar instalaciones con el mismo nivel tecnología; ocasionando incluso problemas de capacidad para atender las operaciones de la empresa que tiene un evento disruptivo.
Sitio móvil	Este tipo de opciones genera mayor valor en aquellos casos en los cuales no se cuenta con servicios de comunicaciones en el área principal en que se encuentra ubicada la organización. Se destacan por su alta capacidad de flexibilidad.	Los recursos y en general los equipos instalados pueden no ser los más adecuados para los lugares en donde se desee implementar el nuevo sitio de operaciones.
Sitio frío	Corresponde a estrategias de bajo costo, rápidas de implementar y sencillas de mantener.	Puede o no tener un alto tiempo de recuperación. Esto dependerá de la complejidad de la tecnología con la que trabaje la Organización. Se

Estrategia	Ventajas	Desventajas
		brinda una falsa sensación de seguridad.
Recuperación y restauración	Son estrategias de bajo costo y fácil de implementar. El foco principal de este tipo de estrategias es la protección contra las pérdidas financieras de activos físicos.	Este tipo de estrategias generalmente no considera los procesos principales del negocio; en razón que no se enfoca en tener un plan para asegurar la continuidad de las operaciones.
Ninguna estrategia	Respuesta menos costosa ante un incidente.	Genera un impacto importante y altos costos para la recuperación.

Fuente: Elaboración propia

Figura 9: Gráfico de costos de implementación de estrategias de continuidad vs tiempo de recuperación



Fuente: Cooperación económica y Técnica (2013). La continuidad de negocios y operaciones frente a situaciones de desastre en América Latina y el Caribe. Balance y recomendaciones.

Tal como se aprecia en la figura 9, el costo de implementar estas estrategias se

encuentra inversamente relacionado con el tiempo de recuperación objetivo. Las estrategias que permiten tener tiempos de recuperación muy cortos – como es el caso de un hot site – requieren de inversiones considerables, sin embargo, permiten tener gran capacidad de respuesta ante eventos disruptivos; por otra parte, aquellas estrategias que tienen tiempos de recuperación más prolongados requieren de menor inversión.

Al respecto, y según la metodología de riesgos, se brindará tratamiento para aquellos que superen un nivel de criticidad 'bajo'. Considerando este aspecto, se obtuvieron todos los riesgos con un nivel de criticidad 'moderado', 'alto' y 'extremo' identificados en la etapa previa (Evaluación de riesgos); y se desarrollaron estrategias que permitan reducir el nivel de riesgo y de esta manera encontrarse dentro del apetito aceptado por la organización (Ver la tabla 42).

Debido a que se encuentra regulada por la SBS, y con el objetivo de cumplir con la circular G-Nº 139, la organización decidió establecer un centro de operaciones y un centro de procesamiento de datos alterno en una de sus sedes de agencia, específicamente en los ambientes de la sede de comas. En el caso del centro de datos alterno, éste cuenta con servidores que replican la información de la base de datos core de forma inmediata. Se ha identificado que el desfase que se tiene en la réplica de la información es de aproximadamente 15 minutos. Por otra parte, en esta misma sede se ha ambientado un espacio para el centro de operaciones alterno, el cual cuenta con equipos que tienen instalados los aplicativos de los sistemas core, y que se encuentran listos para ser utilizados en caso se presente un evento adverso.

Tabla 43: Estrategias para los riesgos identificados

ID	Riesgo	Escenario	Causa	Nivel de Riesgo	Estrategia
RCN - 001	Daños en la infraestructura física de la oficina principal y/o agencias de la organización.	Terremoto	Cambios climatológicos constantes	Moderado	• Establecer un plan de mantenimiento anual, a efectos de identificar las debilidades en infraestructura e instalaciones, a efectos estos aspectos. • Actualizar anualmente los principales activos que deben ser cubiertos por el seguro contra todo riesgo (SCTR). • Elaborar un mapa de distribución de puestos para el centro de operaciones alterno.
		Incendios	Acciones generadas por personas / Cortocircuitos	Alto	
RCN - 002	Daños en el centro de procesamiento de datos	Incendios	Acciones generadas por	Alto	• Establecer un plan de mantenimiento

ID	Riesgo	Escenario	Causa	Nivel de Riesgo	Estrategia
	(CPD) (equipos de comunicaciones, servidores, ambientes de desarrollo, calidad y producción).		personas / Cortocircuitos		anual, a efectos de identificar las debilidades en infraestructura e instalaciones, a efectos estos aspectos. • Actualizar anualmente los principales activos que deben ser cubiertos por el seguro contra todo riesgo (SCTR). • Elaborar un mapa de distribución de puestos para el centro de operaciones alterno.
		Inundaciones	Fallas en los servicios de agua que generen aniego	Alto	
RCN - 003	Indisponibilidad de los servicios de TI (servicio de base de datos, correo, sistema de créditos, sistema de ahorros).	Ciberataques	Continuos ataques informáticos que deterioran o ponen en riesgo los servicios brindados por la organización	Alto	• Establecer un plan de gestión de crisis para los casos en que se presente caída de todos los servicios de TI. • Verificar periódicamente que los sistemas se encuentren actualizados en su última versión. • Establecer planes de respuesta a los incidentes presentados.
		Indisponibilidad del Proveedor	Ausencia de servicios principales, agua	Moderado	• Establecer planes de mantenimiento periódicos para los grupos electrógenos, así como realizar

ID	Riesgo	Escenario	Causa	Nivel de Riesgo	Estrategia
			y electricidad		pruebas constantes a dichos equipos. • Analizar posibles proveedores de servicio de grupos electrógenos para aquellas instalaciones que no cuenten con equipos propios.
RCN - 004	Inaccesibilidad de los trabajadores y clientes a las instalaciones de la organización.	Huelgas / Problemas sociales	Huelgas que ponen riesgo la integridad de las personas y clientes, forzando a cerrar las instalaciones.	Moderado	• Establecer agencias alternas para atención en caso de cierre de alguna agencia / oficina principal
RCN - 005	Ausencia de efectivo en las agencias para atención al cliente.	Indisponibilidad del Proveedor	Indisponibilidad del proveedor para atender las remesas solicitadas por la agencia con déficit de efectivo	Moderado	• Análisis periódico del cumplimiento de los niveles de acuerdo de servicio del proveedor actual. • Analizar y contar con una lista de proveedores alternos que brinden el servicio de remesas en caso de indisponibilidad del actual proveedor.
RCN - 006	Posibles multas y/o	Incendio	Acciones	Alto	• Establecer procesos de digitalización

ID	Riesgo	Escenario	Causa	Nivel de Riesgo	Estrategia
	sanciones debido a pérdida de registros vitales tales como contratos de créditos y ahorros, hojas resumen, cartillas informativas, certificados de desgravamen.		generadas por personas / Cortocircuitos		de documentos (registros vitales).
		Inundaciones	Fallas en los servicios de agua que generen aniego	Alto	
		Errores del personal	Ausencia de personal con el conocimiento y habilidades necesarias para el desarrollo de esta actividad	Moderado	• Establecer planes de capacitación constantes para el personal, y evaluar periódicamente la asimilación de dichas capacitaciones. • Establecer planes de sucesión, identificando claramente a todo el personal clave de cada proceso.

Fuente: Información de la Gerencia de Riesgos de la organización

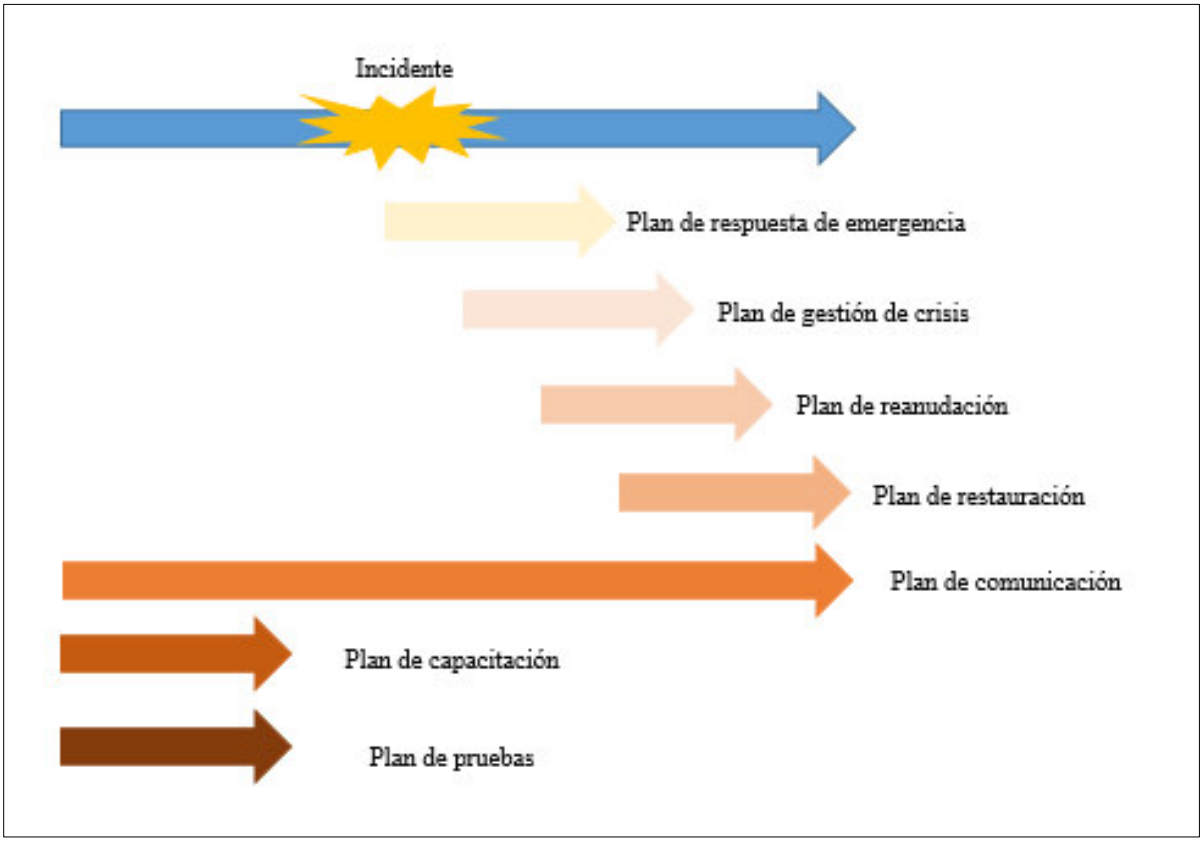
4.10 Planes de continuidad

En esta etapa la organización debe desarrollar e implementar actividades y procedimientos que permitan hacer frente a un evento disruptivo, con el objetivo de reanudar y posteriormente restaurar sus operaciones.

Generalmente las empresas suelen establecer:

- **Plan de respuesta de emergencia**: Este tipo de planes se encuentran orientados a establecer procedimientos para salvaguardar vidas y evitar posibles lesiones. El objetivo principal de este tipo de planes es proteger la vida humana contra cualquier amenaza física.
- **Plan de gestión de crisis**: Estos planes cuentan con procedimientos orientados hacer frente a situaciones complejas, que amenacen la reputación y que pongan en riesgo la existencia de una organización.
- **Plan de recuperación**: Planes que cuentan con procedimientos para reanudar las operaciones críticas de una organización a un nivel aceptable por el cliente.
- **Plan de restauración**: Este tipo de planes son ejecutados inmediatamente luego de los planes de recuperación. Se encuentran orientados a restablecer las operaciones a un nivel normal, es decir, que las operaciones deben regresar a su nivel de operación antes de la ocurrencia del incidente.
- **Plan de comunicaciones**: Conjunto de procedimientos orientados a difundir adecuadamente al personal y al público la situación por la que atraviesa la empresa.
- **Plan de capacitación**: Planes con procedimientos orientados a concientizar y entrenar al personal sobre las acciones a realizar ante un evento disruptivo.
- **Plan de ejercicios y pruebas**: Estos planes establecen procedimientos orientados a probar periódicamente la fortaleza y eficacia del sistema de gestión de continuidad del negocio.

Figura 10: Cronología de activación de los planes de continuidad



Fuente: Elaboración propia

En la figura 10 se pude apreciar el orden con el que se despliega cada uno de los planes del sistema de gestión de continuidad. Tal como se puede ver, el plan de capacitación y de pruebas deben realizarse de forma preventiva, con el objetivo que el personal se encuentre preparado para hacer frente a los eventos disruptivos.

Por otra parte, se debe tener en cuenta que el plan de emergencia, debe ser el primero en desplegarse ante un evento adverso, siempre y cuando dicho evento ponga en riesgo la integridad de física de los trabajadores. En caso el evento adverso genere complicaciones en toda la organización, el siguiente plan a ejecutarse debe ser el de gestión de crisis.

Posteriormente debe ponerse en marca el plan de reanudación que consiste en volver a brindar los productos/servicios bajo niveles aceptables, y finalmente el plan de restauración, con el cual se busca volver a brindar los productos/servicios bajo los estándares normales.

Finalmente cabe indicar que el plan de comunicación debe desplegarse durante todo el sistema de gestión de continuidad.

4.10.1 Plan de respuesta de emergencia

La circular G-Nº139, en su numeral 8.3, establece que las instituciones deben implementar planes de emergencia. Considerando ello, la organización desarrolló un plan de emergencia bajo la estructura que se describe a continuación.

4.10.1.1 Objetivo

Establecer e implementar procedimientos que permita al personal de la organización estar preparados ante situaciones de alto riesgo, tales como desastres naturales o amenazas colectivas que pongan en peligro su integridad física; para lo cual se deben desarrollar acciones rápidas de respuesta.

4.10.1.2 Alcance

Definir el alcance del plan de emergencia, considerando la sede administrativa y las agencias.

4.10.1.3 Roles y responsabilidades

En esta sección del plan, se debe describir claramente los roles y responsabilidades que debe asumir cada uno de los participantes del procedimiento de respuesta ante situaciones de emergencia.

4.10.1.4 Estrategias de respuesta

En esta sección del plan se describe las acciones que se deben de tener en cuenta para los escenarios considerados como emergencia según el análisis – sismos o terremotos, incendios y asaltos. Estas acciones deben de realizarse durante las siguientes etapas:

- Antes: Esta etapa está orientada a definir los criterios de prevención.
- Durante: Esta etapa comprende los procedimientos y criterios para la activación del plan de emergencia y las acciones de respuesta.

- Después: Esta etapa está orientada a identificar las consecuencias que generó la emergencia.

4.10.1.5 Comunicación con instituciones de apoyo externo

En esta etapa se debe identificar y establecer las actividades a implementar para mantener coordinación y comunicación con instituciones externas tales como, la Policía Nacional del Perú, el Cuerpo General de Bomberos voluntarios del Perú, y Defensa Civil, ante situaciones de emergencia.

4.10.1.6 Zonas de evacuación

En el plan de emergencias se deben de señalar cuales son las vías de escape y las zonas seguras. Se deben establecer zonas seguras para que el personal pueda evacuar y esperar durante el periodo que transcurre la emergencia.

4.10.1.7 Desactivación del plan de Emergencia

Finalmente, se debe establecer los responsables de comunicar al personal el término del evento de emergencia, dando por finalizado de esta manera el plan correspondiente.

(ver el detalle del plan de emergencia en el anexo J).

4.10.2 Plan de gestión de crisis

La circular G-Nº139, en su numeral 8.3, establece que las instituciones deben implementar un plan de gestión de crisis. Considerando ello, la organización desarrolló un plan de crisis bajo la estructura que se describe a continuación.

4.10.2.1 Objetivo

Este tipo de planes tiene como finalidad hacer frente a situaciones adversas en su fase más crítica.

Considera la ejecución de un comité de crisis, el cual evalúa la situación y la activación de los planes y estrategias más adecuadas para hacer frente al evento o desastre.

Para ello se describen lineamientos y pautas que debe seguir la organización con la finalidad de mitigar el impacto que podría generar el evento.

4.10.2.2 Alcance

El plan de gestión de crisis es aplicable a toda la organización considerando escenarios o eventos disruptivos en su fase más aguda. Para ello se debe tener en cuenta las estrategias de comunicación.

4.10.2.3 Roles y responsabilidades

En esta sección del plan, se debe describir claramente los roles y responsabilidades que debe asumir cada uno de los participantes del procedimiento en situaciones de crisis. Se deberá contar con el rol que cumple cada uno de los integrantes de este comité.

4.10.2.4 Criterios de invocación y activación

En esta sección del plan se describen todos los criterios y situaciones que se deben considerar para proceder con la activación del plan de gestión de crisis. Se debe tener en cuenta que el despliegue del plan debe realizarse de forma oportuna, motivo por el cual el personal deberá ser capacitado periódicamente respecto a sus funciones a desarrollar.

4.10.2.5 Estrategias y planes de acción

En esta sección del plan se describen las acciones que se deben tener en cuenta para afrontar la crisis de los eventos ocurridos. Estas acciones deben de realizarse durante las siguientes etapas:

- Antes: Esta etapa está orientada a definir los criterios de prevención.
- Durante: Esta etapa comprende los procedimientos y criterios para la activación del plan de crisis y las acciones de respuesta.
- Después: Esta etapa está orientada a identificar las consecuencias que generó el evento las acciones a seguir posterior al término del mismo.

4.10.2.6 Actividades de comunicación

En el plan de gestión de crisis deben establecerse los canales de comunicación y el rol que cumplirán cada uno de los participantes de este plan. Para ello es esencial contar con un árbol de llamadas.

(ver el detalle del plan de gestión de crisis en el anexo K).

4.10.3 Plan de comunicación

4.10.3.1 Objetivo

En este tipo de planes se definen las actividades que permitan contar con un sistema de comunicación efectivo ante la presencia de un evento que genere la interrupción de las operaciones de la organización.

4.10.3.2 Alcance

El plan de comunicaciones está orientado a brindar información sobre el estado de la organización, a sus diferentes grupos de interés; a nivel interno, al personal, familiares y socios; y a nivel externo, a clientes, no clientes, entidades reguladoras, y proveedores.

4.10.3.3 Roles y responsabilidades

En este punto se define la estructura del comité de comunicaciones, el cual tiene relación directa con el comité de crisis. Ello debido a que la función del coordinador de comunicaciones (líder del comité de comunicaciones) es realizada por la Gerencia General, quien también responsable de dirigir el comité de crisis.

4.10.3.4 Activación

El plan de comunicaciones se activa como parte de la ejecución de una situación de crisis. Este plan debe contar con tres fases para su despliegue:

- Fase Antes – Actividades de preparación: Esta fase está orientada a mantener actualizada las listas de contactos, así como verificar que los recursos a utilizar durante la ejecución del plan se encuentren disponibles.
- Fase Durante – Actividades de activación y respuesta: En esta fase se debe esperar por el análisis realizado por el comité de crisis, el cual decidirá el alcance de las comunicaciones a realizar (accionistas,

personal, familiares, clientes, prensa).

- Fase Después – Actividades de desactivación: En esta fase se espera recibir notificación del comité de crisis para proceder con la desactivación del plan de comunicaciones, y posteriormente realizar un informe determinando el impacto a nivel de imagen que se obtuvo como consecuencia de la crisis.

(ver el detalle del plan de comunicación en el anexo L).

4.10.4 Plan de recuperación de desastres

La circular G-Nº139, en su numeral 8.3, establece que las instituciones deben implementar un plan de recuperación de los servicios de tecnología de información. Considerando ello, la organización desarrolló un plan de crisis bajo la estructura que se describe a continuación.

4.10.4.1 Objetivo

Este plan tiene por objetivo restaurar los servicios que brinda el área de tecnología de información, los cuales soportan procesos críticos de la organización.

4.10.4.2 Alcance

El alcance del presente plan abarca a todos los trabajadores del departamento de tecnología de información y que participan en las actividades de levantamiento, configuración y administración de los servicios de TI, los cuales brindan soporte a los procesos críticos de la organización.

4.10.4.3 Roles y responsabilidades

En este apartado se definen las funciones de los trabajadores del equipo de TI encargados de los servicios que soportan los procesos críticos de la organización.

4.10.4.4 Revisión y actualización

El plan de recuperación de desastres de TI debe contar con criterios para su

actualización periódica, así como establecer el responsable de realizar dicha actualización.

4.10.4.5 Estrategias

El plan de recuperación de desastres de TI (DRP), considera tres fases:

- Fase Antes: Esta etapa se encuentra orientada a la verificación de hardware y estructura lógica de las instalaciones del centro de datos principal y alterno.
- Fase Durante: En esta etapa se definen las actividades a desarrollar como respuesta a los eventos ocurridos. Se debe tener en cuenta que las actividades de reanudación de las operaciones deben considerar los tiempos establecidos en el análisis de impacto (BIA).
- Fase Después: Se establecen las actividades que permitan el retorno a la normalidad de los servicios que brinda el departamento de TI (comunicaciones, sistemas de información, bases de datos, active directory, accesos, seguridad perimetral, entre otros).

4.10.4.6 Mantenimiento del plan y Pruebas

El plan de recuperación de desastres debe contar con pruebas detalladas. Las pruebas permitirán identificar errores y establecer estrategias que permitan tener tiempos óptimos y de esa forma no superar los RTO definidos. Estas pruebas pueden definir en el plan de pruebas general, siempre y cuando incluyan todos los servicios de TI.

(ver el detalle del plan de recuperación de desastres en el anexo M).

4.10.5 Plan de capacitación

4.10.5.1 Objetivo

El plan de capacitación tiene como objetivo capacitar y concientizar al personal y a los diferentes integrantes de cada comité (emergencia, crisis, comunicaciones, contingencia, recuperación de desastres) respecto a sus funciones a desarrollar.

4.10.5.2 Alcance

La capacitación debe considerar la concientización al nivel de toda la organización, tanto para el personal de la oficina principal como para las agencias.

4.10.5.3 Desarrollo

El plan de capacitación debe desarrollarse de forma periódica, mínimamente con frecuencia anual, y debe considerar el universo del personal de la organización.

Este plan será elaborado por el analista de continuidad del negocio y será aprobado por el Comité de Riesgo operacional, continuidad del negocios y seguridad de la información.

4.10.6 Plan de pruebas

4.10.6.1 Objetivo

Establecer procedimientos que permitan verificar la eficacia de los diversos planes, asegurando de esta forma un adecuado nivel de respuesta ante situaciones de riesgo para la continuidad de las operaciones.

4.10.6.2 Alcance

Este plan es aplicable a todos los planes de del sistema de gestión de continuidad del negocio, así como a todos los trabajadores que intervienen en el proceso de ejecución de pruebas.

4.10.6.3 Desarrollo

El despliegue de las pruebas debe considerar tres criterios: tiempo, recursos y conocimiento.

- Uno de los objetivos principales de las pruebas es verificar que los tiempos de recuperación sean menores a los RTO definidos.
- Se debe verificar que los recursos se encuentren disponibles (activos de

información, infraestructura, personal, proveedores, entre otros).

- Se debe verificar que los miembros cuenten con el conocimiento suficiente para el desarrollo de sus actividades.

Este plan cuenta con cuatro etapas:

a) Establecimiento de las bases: En esta primera etapa se deberá elaborar el plan anual de pruebas, el cual debe ser aprobado por el comité de riesgos, y se deberá considerar qué planes de continuidad se evaluarán.
b) Planificación, diseño y desarrollo: En esta etapa se deberá coordinar con el personal correspondiente para llevar a cabo la ejecución de las pruebas, así como verificar la disponibilidad de la infraestructura y recursos necesarios. Finalmente se deberá coordinar la participación de veedores en caso se requiera.
c) Etapa de ejecución: En esta etapa se realizará la ejecución de las pruebas, debiendo registrarse las incidencias que pudieran presentarse durante la ejecución de las mismas.
d) Etapa de mejora continua: En esta etapa se deberá realizar un informe con el resultado de las pruebas, identificando los incidentes presentados durante las mismas, con el objetivo de establecer estrategias que permitan superar dichos incidentes en pruebas futuras.

4.11 Pruebas del sistema de gestión de continuidad

En esta etapa, se debe realizar pruebas orientadas a verificar el adecuado funcionamiento del sistema de continuidad, simulando eventos que puedan poner en riesgo la entrega de los productos o servicios críticos previamente definidos.

Estas pruebas generalmente se encuentran orientadas a validar el correcto funcionamiento de equipos y la tecnología que se utiliza en la organización para los procesos críticos.

La organización considera en su metodología los siguientes tipos de pruebas:

- **Pruebas estáticas o de verificación**: Este tipo de pruebas están orientadas a verificar la existencia de los equipos y recursos, este tipo de prueba es la más débil, ya que solo se verifica que se cuente con los recursos, no se comprueba el funcionamiento de los mismos.
- **Pruebas funcionales**: Estas pruebas está orientadas a verificar que los equipos y/o recursos funcionen para el propósito señalado. Durante estas pruebas se verifica que, en el caso de equipos informáticos, éstos cuenten con las aplicaciones necesarias para llevar a cabo los procesos críticos.
- **Prueba de escritorio**: Para este tipo de prueba, se debe reunir al personal responsable de cada actividad de los planes de continuidad, y se deberá verificar el despliegue de dicho plan. El desarrollo de esta prueba está orientada a verificar el conocimiento de cada uno de los participantes respecto a sus actividades específicas.
- **Prueba parcial**: Este tipo de pruebas busca verificar que el plan de continuidad de un determinado proceso o área funcione de forma correcta.
- **Prueba Operacional completa**: Esta prueba es la de mayor alcance, y por lo tanto la de mayor complejidad. Este tipo de pruebas considera simulaciones de eventos reales, sin afectar las operaciones del día a día de la organización.

En el periodo 2018 en la organización se realizaron todos los tipos de pruebas descritos anteriormente. Sin embargo, cabe indicar que el tipo de prueba operacional completa fue la más adecuado para medir y comparar los tiempos de recuperación reales y los tiempos de recuperación teóricos.

Durante las diferentes pruebas, se simularon escenarios de incendios, sismos, robos,

ataques informáticos; los cuales generaron supuestos tales como indisponibilidad de servicios eléctricos, servicios de telecomunicaciones (redes), servicios de base de datos, indisponibilidad de personal y otros.

En la figura 4.5 se muestra la comparación de los tiempos de recuperación y del periodo máximo tolerable, teniendo en cuenta los aspectos detallados en la tabla 43:

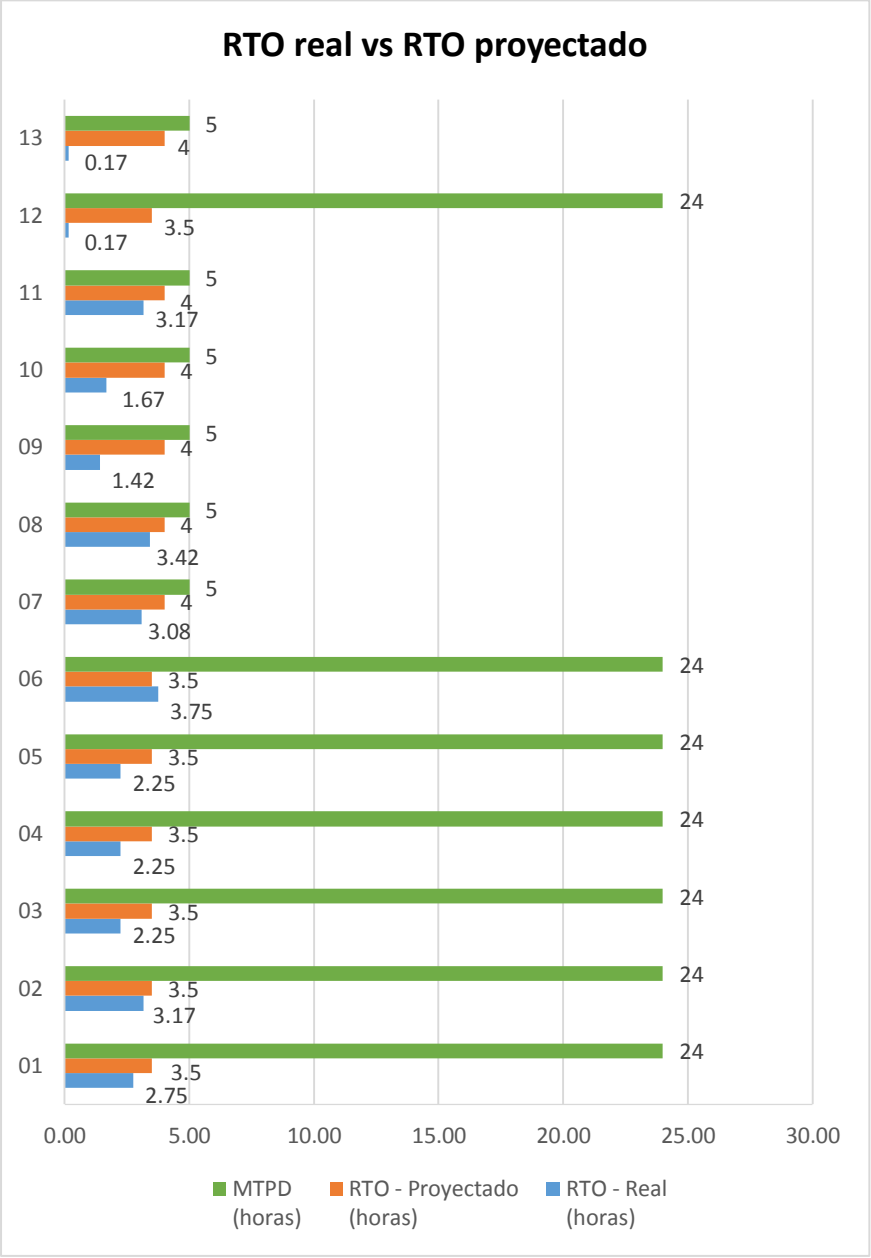
Tabla 44: Tiempos de recuperación objetivo real, proyectado y tiempo de recuperación tolerable

Nro.	Descripción	RTO - Real (horas)	RTO - Proyectado (horas)	MTPD (horas)
01	Recuperación del sistema de créditos - indisponibilidad de base de datos	2.75	3.5	24
02	Recuperación del sistema de créditos - indisponibilidad de la red	3.17	3.5	24
03	Recuperación del proceso de evaluación de clientes - indisponibilidad de personal	2.25	3.5	24
04	Recuperación del proceso de aprobación de créditos - indisponibilidad de personal	2.25	3.5	24
05	Recuperación del proceso de desembolso de créditos - indisponibilidad de personal	2.25	3.5	24
06	Recuperación del proceso de canales de atención	3.75	3.5	24
07	Recuperación del sistema de pasivos - indisponibilidad de base de datos	3.08	4	5
08	Recuperación del sistema de pasivos - indisponibilidad de la red	3.42	4	5
09	Recuperación del proceso de fondeo por depósitos del público - indisponibilidad de personal	1.42	4	5
10	Recuperación del sistema de consultas y reclamos - indisponibilidad de base de datos	1.67	4	5
11	Recuperación del sistema de consultas y reclamos - indisponibilidad de la red	3.17	4	5

Nro.	Descripción	RTO - Real (horas)	RTO - Proyectado (horas)	MTPD (horas)
12	Recuperación de sistema de créditos - indisponibilidad de electricidad	0.17	3.5	24
13	Recuperación de sistema de pasivos - indisponibilidad de electricidad	0.17	4	5

Fuente: Resultados de pruebas de la organización – Elaboración propia

Figura 11: Comparación de tiempo de RTO y MTPD



Fuente: Elaboración propia

Como se pudo apreciar en la tabla 43; el tiempo de recuperación del proceso de canales de atención superó el RTO teórico, y si bien no superó el MTPD; debe establecerse planes de acción que permitan reducir el RTO y así mantener los niveles de apetito definidos por el Directorio.

Por otra parte, en la figura 11, se aprecia que en ninguna de las pruebas el tiempo objetivo de recuperación ha superado el periodo máximo de interrupción tolerable (MTPD); sin embargo, si se ha superado el RTO teórico en una de las pruebas, por lo que en dicho caso deberá evaluarse actualizar dicho valor o ejecutar planes de acción que permitan disminuir dicho RTO.

4.12 Auditoría del sistema de gestión de continuidad del negocio

La circular G-Nº 139, en su artículo 11º establece que la unidad de auditoría interna debe evaluar el cumplimiento de dicha circular.
Para ello, la Gerencia de Auditoría Interna deberá considerar en su plan anual de trabajo, la evaluación al sistema de gestión de continuidad del negocio de la organización.

En esta etapa se desarrollará un programa de auditoría, el cual debe estar orientado en cumplir con los diferentes aspectos descritos en la ISO 22301. Las evaluaciones de auditoría deben considerar en sus informes como mínimo los aspectos definidos en el artículo 22º de la resolución SBS Nº 11699-2008, y adicionalmente, podrán considerar también como buenas prácticas, los apartados descritos en la ISO 19011 – Directrices para la auditoría de sistemas de gestión.

A continuación, se presenta la tabla 44, en la cual se muestra el programa de auditoría:

Tabla 45: Programa de Trabajo – Auditoría al Sistema de Gestión de Continuidad del Negocio

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
4. Contexto de la organización		- **Artículo 8º (8.1)** - Entendimiento de la Organización (Considera análisis de impacto y evaluación de riesgos)	Puntaje de cumplimiento: 2.0	- Verificar que la organización cuente con un Sistema de Gestión de Continuidad del Negocio, en el cual se haya establecido: * el alcance del SGCN * los requisitos de partes interesadas * los objetivos del SGCN - Verificar que los objetivos del SGCN se encuentren alineados a la misión, visión, y objetivos establecidos en el plan	- Se identificó que el SGCN no tiene claramente definido el alcance, debido a que no se tenía identificado los productos sobre los cuales se iba aplicar la continuidad. - Se identificó que algunos objetivos del SGCN no se encontraban alineados a los objetivos establecidos en el plan	No se identificaron hallazgos.
4.1 Entendimiento de la organización y de su contexto	2					
4.2 Entendimiento de las necesidades y expectativas de las partes interesadas	2					
4.3 Determinación del campo de aplicación del sistema de gestión de la continuidad del negocio	2					
4.4 Sistema de gestión de la continuidad del	2					

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
negocio				estratégico.	estratégico.	
5. Liderazgo		- **Artículo 4º** - Responsabilidad del Directorio - **Artículo 5º** - Responsabilidad de la Gerencia - **Artículo 6º** - Responsabilidad de la unidad de riesgos - **Artículo 7º** - Función de la continuidad del	Puntaje de cumplimiento: 2.0	- Verificar la existencia de una política de continuidad del negocio, en la cual se establezcan las funciones y responsabilidades de los participantes en el SGCN. - Validar que los estatutos, normas y procedimientos que definen el SGCN se encuentren aprobados por el Directorio y el comité correspondiente.	- Se identificó que la política fue actualizada en el mes de mayo 2017, sin embargo, estos cambios no fueron presentados y aprobados en la sesión de Directorio correspondiente. - Se identificó que en normas internas no se	No se identificaron hallazgos.
5.1 Liderazgo y compromiso	2					
5.2 Compromiso de la dirección	2					
5.3 Política	2					

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
5.4 Funciones, responsabilidades y autoridad en la organización	2	negocio		- Verificar la conformación de un comité de CN, aprobado por el Directorio. - Verificar la adecuada ejecución del comité de CN, a través de la revisión de actas y el seguimiento de acuerdos.	establecieron las funciones y responsabilidades de la Gerencia General y la Gerencia de Riesgos.	
6. Planificación			Puntaje de cumplimiento: 2.0	- Verificar que el SGCN cuente con una metodología de gestión de riesgos (identificación, evaluación y tratamiento). - Verificar que las normas y	- Se identificó que para un grupo de riesgos no se ha establecido los planes de acción correspondientes; por otra parte, también se	No se identificaron hallazgos.
6.1 Acciones para cubrir riesgos y oportunidades	2					

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
6.2 Objetivos de continuidad del negocio y planes para conseguirlos	2			procedimientos del SGCN se encuentren alineadas a la gestión de riesgos de la organización. - Verificar la identificación, evaluación y tratamiento de riesgos en función a la metodología de riesgos de la organización. - Verificar que los objetivos del SGCN se encuentren alineados a la política de continuidad.	identificaron riesgos con planes de acción que carecían de fecha de implementación.	
7. Apoyo		- **Artículo 9º** -	Puntaje de cumplimiento:	- Verificar que la unidad de	- Si bien se identificó	- Se

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
7.1 Recursos	2	Documentación sustentatoria - **Artículo 8º (8.5)** - Integrar la gestión de la continuidad del negocio a la cultura organizacional	1.8	continuidad de continuidad cuente con un presupuesto detallado para la gestión de continuidad del negocio. - Verificar que los puestos (asistentes, analistas, jefaturas) para el ejercicio del SGCN se encuentren cubiertos. - Solicitar los currículums de los trabajadores responsables del SGCN y verificar que cuenten con la	que se tiene un importe para la gestión de continuidad, no se aprecia que este presupuesto se encuentre detallado (el importe que será designado a capacitaciones, a pruebas periódicas, en adquisición de herramientas, etc.) - Se identificó que un	identificó que no se cuenta con el universo de incidentes ocurridos. En la herramienta Aranda no se registraron los incidentes ocurridos en
7.2 Competencia	2					

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
7.3 Concienciación	2			experiencia suficiente para el ejercicio de sus funciones. - Verificar que la política sea difundida a toda la organización. - Verificar que se cuente con mecanismos de difusión y capacitación para todo el personal, respecto al tema de continuidad del negocio. - Solicitar y verificar el cumplimiento de un plan de	analista de continuidad, no cuenta con el conocimiento exigido según su ficha de funciones. - Se identificó que los incidentes son comunicados a partir del usuario final, no se cuentan con herramientas para la identificación de incidentes, así como tampoco se gestiona el registro de dichos	el periodo de diciembre 2017 a febrero 2018.
7.4 Comunicación	1					
7.5 Información documentada	2					

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
				capacitación referido a temas de continuidad del negocio. - Verificar que se cuente con un plan de comunicaciones. - Verificar que se cuente con mecanismos de comunicación ante el suceso de eventos o incidentes. - Identificar todos los documentos normativos referidos al SGCN, y	incidentes. - Se identificó que el servidor en el cual se almacenan los documentos normativos vigentes, no forma parte de los procedimientos de respaldo. Por otra parte se identificaron documentos que no se encontraban vigentes, sin embargo estaban disponibles para el uso de los trabajadores.	

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
				verificar, que se encuentren vigentes, que cuenten con control de versiones, que sea accesible a todo el personal, y que sea resguardado.		
8. Operación		- **Artículo 8º (8.2)** - Entendimiento de la Organización (Considera selección de estrategia de	Puntaje de cumplimiento: 1.8	- Verificar que se cuente con un procedimiento formal para la elaboración del análisis de impacto al negocio (BIA)	- Se identificó que se realizaba el BIA a partir de los procesos, sin identificar los productos y servicios críticos que brinda la organización.	- Se identificó que algunos equipos del sitio alterno de operaciones no contaba
8.1 Planificación y control operacional	2					

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
8.2 Análisis de impacto en el negocio y apreciación del riesgo	2	continuidad, y la ejecución de pruebas)		- Verificar que el BIA incluya: * la identificación de productos y servicios críticos, considerando la evaluación del impacto que genera no otorgar dichos productos/servicios * tiempos para recuperación de las operaciones, considerando un nivel mínimo aceptable * las dependencias, los recursos necesarios, y los proveedores involucrados en los procesos orientados a otorgar productos y	- Se identificó que no se tiene formalizado la frecuencia de ejecución del BIA. - Se identificaron riesgos con criticidad 'alto' que no contaban con un plan de mitigación.	con algunos aplicativos necesarios para la ejecución de operaciones de forma regular.

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
				servicios * asimismo, deberá indicarse la frecuencia de ejecución del BIA		

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
8.3 Estrategia de continuidad del negocio	1			- Verificar que se cuente con un procedimiento formal para la identificación, evaluación y tratamiento de riesgos, considerando que debe tener un nivel de priorización tanto para la evaluación como para el tratamiento de éstos. - Verificar que las estrategias de continuidad se encuentren acorde con la capacidad de la organización, que se encuentren aprobadas por	- Se identificó que el sitio alterno de operaciones, contaba con equipos no operativos, por otra parte, algunos equipos no contaban con los aplicativos necesarios para la ejecución de operaciones. - Se identificaron que algunas normas (reglamentos o políticas) no se encontraban aprobadas por el nivel	

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
				el nivel correspondiente, y que contribuyan a la mitigación de los riesgos. - Verificar que se cuente con un sitio alterno de operaciones listo para ser utilizado ante eventos disruptivos.	correspondiente.	

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
8.4 Establecimiento e implantación de procedimientos de continuidad del negocio	2			- Verificar que cada una de las fases del SGCN se encuentre documentada y formalizada en reglamentos, normas, procedimientos; así como también aprobados por el nivel correspondiente. - Verificar que se cuenten con planes de continuidad documentados, aprobados y actualizados (plan de emergencia, plan de gestión de crisis, plan de comunicaciones, plan de	- Se identificó que no se tiene pruebas integrales (pruebas que consideren la activación en secuencia de los diferentes planes, plan de emergencia, plan de crisis, plan de recuperación). - Se identificó que no se ejecutaron un grupo de pruebas planificadas para el periodo 2017.	

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
				recuperación) - Verificar que los proveedores críticos cuenten con planes de continuidad del negocio. - Verificar que se cuente con un plan de pruebas, el cual se encuentre orientado a verificar la efectividad de todos los procedimientos de continuidad.		

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
8.5 Pruebas y ensayos	2			- Verificar que se establezca en normas internas la frecuencia con la que se debe realizar las pruebas de continuidad - Verificar que los resultados de las pruebas realizadas se formalicen en un informe, el cual deberá ser presentado a los niveles correspondientes (Directorio, Gerencia General, Gerencia de Riesgos)	- Se identificó que un proveedor crítico no cuenta con planes de continuidad.	
9. Evaluación y medición del rendimiento		- **Artículo 10º** - Cambios	Puntaje de cumplimiento: 2.0	- Verificar que el personal responsable de la unidad de	- Se identificó que la unidad de continuidad	No se identificaron

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
9.1 Supervisión, medición, análisis y evaluación	2	significativos - **Artículo 11º** - Auditoría interna		continuidad, evalúe periódicamente la efectividad del sistema - Verificar que la organización cuente con un procedimiento para identificar los cambios significativos. - Verificar que el plan anual de la Gerencia de Auditoría Interna, considera una evaluación al SGCN - Verificar que los cambios	no realizó el total de pruebas en el periodo 2017 - Se identificó que los resultados de las pruebas realizadas en el periodo 2017, no se presentaron en sesión de Directorio	hallazgos.
9.2 Auditoría interna	2					
9.3 Revisión de la dirección	2					

Norma ISO 22301	Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
			normativos que correspondan sean aprobados por el Directorio - Verificar que las estrategias, planes de continuidad y planes de pruebas sean aprobados por el directorio - Verificar que los resultados de las pruebas sean de conocimiento del Directorio		
10. Mejora		Puntaje de cumplimiento:	- Verificar que las acciones	- Se identificaron	No se

Norma ISO 22301		Norma SBS G-Nº 139	Nivel de cumplimiento (2018): (0) No cumple, (1) Cumple Parcialmente, (2) Cumple	Procedimiento Auditoría	Auditoría 2017	Auditoría 2018
10.1 No conformidad y acción correctora	2		2.0	correctoras y las recomendaciones de auditoría (interna, externa y SBS) en materia de continuidad del negocio, cuenten con fecha de implementación	recomendaciones de auditoría que no fueron implementadas de forma oportuna, y sobre las cuales no se cuenta con un sustento sólido respecto a su retraso	identificaron hallazgos.
10.2 Mejora continua	2					

Fuente: Informes de Auditoría de los periodos 2017 y 2018

Figura 12: Comparación del nivel de cumplimiento de la norma ISO 22301 – Antes y después de la implementación

Fuente: Elaboración propia

En la figura 12, se puede apreciar que el nivel de cumplimiento respecto al sistema de gestión de continuidad del negocio es aproximadamente el 100% en cada uno de los apartados de la ISO 22301.

V. ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

5.1 Presentación de resultados

5.1.1 Análisis de impacto al negocio (BIA)

En el marco de la implementación del sistema de gestión de continuidad del negocio basado en la norma ISO 22301, en la organización se identificaron nueve tipos de productos, los cuales se pueden apreciar en el numeral 4.7.1.

A través de la metodología de impactos definida en la guía técnica ISO 22317 se determinó que los productos críticos son créditos y ahorros. Para mayor detalle ver tabla 7 y tabla 8.

Por otra parte, se identificaron 64 procesos (ver anexo C), de los cuales 23 se encuentran relacionados a los productos críticos (ver tabla 9), determinando a través de la metodología de impactos 06 procesos críticos para la organización, los cuales se pueden apreciar en la tabla 10.

En la tabla 46 se puede apreciar la interrelación de los procesos críticos y los productos críticos de la organización, sobre los cuales se implementó todo el sistema de gestión de continuidad.

Tabla 46: Relación de procesos críticos y productos críticos

Proceso Crítico	Producto crítico asociado
Evaluación	Créditos
Aprobación	Créditos
Desembolso	Créditos
Fondeo por depósitos del público	Ahorros
Administración de canales de atención	Créditos y Ahorros
Atención al cliente	Créditos y Ahorros

Fuente: Elaboración propia

5.1.2 Identificación y análisis de riesgos

En la etapa de gestión de riesgos, se determinaron diez escenarios o amenazas, y sobre ellos se identificaron siete riesgos claves que pueden afectar la continuidad de las operaciones de la organización. Teniendo en cuenta el nivel de apetito al riesgo, se

establecieron controles sobre aquellos riesgos con nivel de riesgo residual moderado, alto y extremo. El detalle del análisis de riesgos se puede apreciar en la tabla 39 y en la tabla 42.

5.1.3 Planes de continuidad del negocio

En el marco de la implementación del sistema de gestión de continuidad del negocio basado en la norma ISO 22301, se determinaron mecanismos de respuesta a eventos disruptivos, estableciendo 07 tipos de planes de continuidad, teniendo en cuenta que 02 de estos tipos de planes (plan de capacitación y plan de pruebas) son de carácter preventivo y 05 planes (plan de respuesta de emergencia, plan de gestión de crisis, plan de reanudación y plan de restauración) de carácter correctivo.

Para mayor detalle se pueden apreciar los planes en los anexos J, K, L, M.

5.1.4 Auditoría

Como parte de la implementación del sistema de gestión de continuidad del negocio, se realizó una auditoría en el año 2018, a efectos de verificar el incremento en el cumplimiento de cada uno de los apartados de la ISO 22301. Los resultados permitieron verificar que se tiene un cumplimiento en cinco apartados de un total de siete apartados definidos en la ISO 22301. El detalle del cumplimiento se puede apreciar en la tabla 44 y en la figura 12

Tabla 47: Incremento del cumplimiento de la ISO 22301

Apartado	Puntaje - 2017	Puntaje - 2018	% incremento de cumplimiento
4. Contexto de la Organización	1.5	2.0	25%
5. Liderazgo	1.5	2.0	25%
6. Planificación	1.5	2.0	25%
7. Apoyo	1.2	1.8	33%
8. Operación	1.2	1.8	33%
9. Evaluación del Rendimiento	1.3	2.0	25%
10. Mejora	1.5	2.0	25%

Fuente: Elaboración propia

5.2 Contrastación de hipótesis

5.2.1 Contrastación de hipótesis general

Ho: La implementación de un sistema de gestión de continuidad del negocio basado en la norma ISO 22301 no evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

Ha: La implementación de un sistema de gestión de continuidad del negocio basado en la norma ISO 22301 no evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

De los resultados que se muestran en el análisis de impacto, la gestión de riesgos, los planes de continuidad y el proceso de auditoría, se puede evidenciar que la implementación de un sistema de gestión de continuidad del negocio basado en la ISO 22301 sí evidencia la capacidad de la organización para continuar brindando sus productos y/o servicios antes situaciones disruptivas.

5.2.2 Contrastación de hipótesis específica 1

Ho: El análisis de impacto al negocio no evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

Ha: El análisis de impacto al negocio sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

Se clasificaron los productos de la organización según sus características, teniendo un total de nueve tipos de productos. Sobre estos productos se realizó un análisis de impacto, considerando la guía técnica ISO 22317, determinando que el sistema de gestión de continuidad se establecerá sobre dos productos críticos, que son créditos y ahorros. Posteriormente, considerando el catálogo de procesos, se identificaron aquellos procesos relacionados a los productos críticos y se realizó un análisis de impacto sobre estos procesos, determinando 06 procesos críticos, los cuales deben ser restablecidos ante situaciones disruptivas, para ello se logró identificar el tiempo objetivo de recuperación, así como el tiempo límite que puede permanecer

la organización sin operar por un tiempo determinado.
Los resultados permiten concluir que el análisis de impacto sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

5.2.3 Contrastación de hipótesis específica 2

Ho: La implementación de la gestión de riesgos de la norma ISO 22301 no evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

Ha: La implementación de la gestión de riesgos de la norma ISO 22301 sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

Del análisis realizado, se evidencia que la matriz de riesgos permite determinar los controles necesarios para mitigar los riesgos de continuidad a los que se encuentran expuestos los procesos críticos de la organización; considerando que estos riesgos deben mantenerse dentro del nivel de apetito de riesgo de la empresa, el cual se ha establecido en S/ 61 mil.
El presente análisis evidencia que la identificación y análisis de riesgos influye positivamente en evidenciar la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

5.2.4 Contrastación de hipótesis específica 3

Ho: Establecer planes de continuidad del negocio no evidencian la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

Ha: Establecer planes de continuidad del negocio influye sí evidencian la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

Los planes de continuidad establecen el procedimiento paso a paso que se debe desarrollar a efectos de poder restablecer un proceso en un tiempo determinado; debido a ellos se realizaron pruebas operacionales completas con el objetivo de verificar que los planes de recuperación se ejecuten dentro del tiempo proyectado. En la tabla 44 se tienen los tiempos reales de recuperación que tuvieron los procesos críticos, pudiendo apreciar que en ninguno de los casos se superó el tiempo límite identificado en la etapa de análisis de impacto.

Este análisis permite concluir que el establecimiento de planes de continuidad sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

5.2.5 Contrastación de hipótesis específica 4

Ho: La ejecución de auditorías no evidencian la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

Ha: La ejecución de auditorías sí evidencian la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

Las auditorías permiten verificar el nivel de cumplimiento que tiene una organización respecto a un tema en específico. Del análisis realizado en la presente investigación se aprecia que la empresa tiene un nivel de cumplimiento completo en cinco de siete aparatados implementables de la norma ISO 22301, lo cual permite afirmar que la organización se encuentra preparada para responder a eventos adversos a través del uso de esta metodología.

Este análisis permite concluir que la ejecución de auditorías sí evidencia la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

5.3 Discusión de resultados

Los resultados que se muestran en la presente tesis, evidencian que el análisis de impacto (BIA), la gestión de riesgos, los planes de continuidad y la ejecución de

auditorías permiten demostrar que la implementación de un sistema de gestión de continuidad del negocio basado en la norma ISO 22301, sí evidencian la capacidad de la organización para continuar brindando productos y/o servicios ante situaciones disruptivas

VI. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- El resultado de la presente investigación permite evidenciar que la organización cuenta con la capacidad para continuar brindando sus servicios y/o productos ante eventos disruptivos, en el marco de la norma ISO 22301.

- El análisis de impacto de la norma ISO 22301, permitió identificar los productos y procesos críticos de la organización, y sobre ellos fue posible implementar el sistema de gestión de continuidad. La implementación se realizó sobre el 22% de productos, en razón que éstos representan el 89% de la utilidad de la empresa.

- La etapa de gestión de gestión de riesgos de la ISO 22301, permitió la identificación de los riesgos que amenazan la continuidad de los procesos críticos de la organización, con el objetivo de establecer controles sobre aquellos riesgos que superen el nivel de criticidad permitido según el Directorio, el cual fue estimado en S/ 61 mil. Se identificó que, de un total de 10 escenarios de continuidad, 07 son aplicables para la organización.

- El establecimiento de planes de continuidad, permitió contar con procedimientos detallados que permitan recuperar la operatividad de los procesos críticos de la organización en un tiempo adecuado, que no genere pérdidas significativas para la empresa.

- La ejecución de auditorías permite identificar debilidades, oportunidades de mejora, así como el nivel de cumplimiento de la organización con respecto al sistema de gestión de continuidad del negocio en el marco de la norma ISO 22301. En el presente estudio se determinó que la organización cumple con 5 aparatados de los 7

establecidos en el estándar en mención.

- El análisis realizado en la etapa de contexto de la organización, permitió identificar las brechas que tenía la empresa con respecto a los apartados señalados en la ISO 22301.

- Como parte del análisis de impacto al negocio (BIA operativo), se identificaron las actividades que soportan la ejecución de procesos críticos, lo que permitió identificar proveedores claves, procesos soporte, personal clave, sistemas de información, equipos, registros clave y otros recursos necesarios para la ejecución del proceso.

- Las pruebas operacionales completas realizadas en el periodo 2018, permiten evidenciar el correcto funcionamiento de los planes de continuidad, debido a que los tiempos de recuperación reales son menores a los tiempos de recuperación teóricos establecidos para cada uno de los procesos.

6.2 Recomendaciones

- Si bien, el modelo de implementación de la presente tesis es recomendable para todas las entidades del sistema microfinanciero; es importante indicar que todo el sistema de gestión de continuidad de la norma ISO 22301 puede ser aplicable para cualquier organización; independientemente del sector al cual correspondan.

- El SGCN debe ser implementado por personal con conocimiento en el tema; con el objetivo de garantizar un adecuado proceso.

- Se recomienda analizar el ámbito externo constantemente, e identificar nuevos riesgos que podrían conllevar a la paralización de las operaciones de la organización.

- Se recomienda que el personal partícipe en cada uno de los planes de continuidad, sea capacitado frecuentemente respecto a las funciones que desarrollará; ello con el objetivo de responder de forma óptima ante eventos disruptivos; y no poner en

riesgo las actividades de respuesta, reanudación y recuperación.

- Involucrar activamente al Directorio como parte del Sistema de Gestión de Continuidad del Negocio; considerando que no solo debe enviarse informes para conocimiento.

- Los programas de auditoría pueden modificarse y ser más exigentes en cuanto al cumplimiento de la norma ISO 22301, a medida que la organización adquiera mayor madurez con respecto a este sistema de gestión.

- Se recomienda que la organización realice un análisis de costo-beneficio, que permita determinar las ventajas y el valor agregado que otorga una certificación internacional, como es el caso de la ISO 22301.

BIBLIOGRAFÍA

Ahrens, S. et al. (2005). *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery.* United States of America: ASIS International.

Arias Bailly, B. (2016). *Simulación como parte de la gestión de crisis*. Lima-Perú: Universidad Nacional Mayor de San Marcos. Obtenido de http://cybertesis.unmsm.edu.pe/handle/cybertesis/5666

BCI. (2007). *Business Continuity Institute Good Practice Guidelines 2007: A Management Guide to Implementing Global Good Practice in Business Continuity Management*. Madrid: Emelar Grafic, S.L.

BCI. (2018). *BCI Continuity and Resilience Report 2018. Raising the impact of Business Continuty*.Obtenido de: https://www.b-c-training.com/img/uploads/resources/9e2f6409-da19-4c4a-a8a8d58733a08d4f.pdf

BCI. (2018). *Horizon Scan Report 2018*. Obtenido de: https://www.bsigroup.com/es-PE/gestion-de-la-continuidad-del-negocio-iso-22301-/reporte-horizon-scan-2018/

Belaunde G. (2013). *Riesgos empresariales ligados a "Desastres Naturales": una visión integral*. Obtenido de https://gestion.pe/blog/riesgosfinancieros/2013/04/riesgos-empresariales-ligados.html

Belaunde, G. (2014). *Continuidad Operativa o del Negocio - Ejemplos de éxito*. https://gestion.pe/blog/riesgosfinancieros/2014/09/continuidad-operativa-o-del-negocio-ejemplos-de-exito.html

Castillo Aparicio, C. (2014). *Modelo de análisis de impacto en el negocio para el desarrollo de la continuidad de negocio aplicable a empresas del sector financiero*. Lima-Perú: Universidad Nacional de Ingeniería. Obtenido de http://cybertesis.uni.edu.pe/handle/uni/7277

Castro Marquina, L. (2013). *Diseño de un sistema de gestión de continuidad de negocios (SGCN) para la RENIEC bajo la óptica de la norma ISO/IEC 22301*. Lima-Perú: Pontificia Universidad Católica del Perú. Obtenido de http://tesis.pucp.edu.pe/repositorio/handle/123456789/5110

Collier, B. (2018). *¿Qué pasa con las pequeñas y medianas empresas tras un desastre natural?* Obtenido de https://www.marsh.com/uy/es/insights/research/-que-pasa-con-las-pequenas-y-medianas-empresas-tras-un-desastre-.html

Comunidad Andina. (2009). *Atlas de las dinámicas del territorio andino: Población y bienes expuestos a amenazas naturales*. Obtenido de http://www.comunidadandina.org/predecan/doc/libros/atlas.pdf

COSO. (2013). *Control Interno – Marco Integrado Marco y Apéndices*.

Dergarabedian, C. (2011). *Los ataques del "11-S" y el fuerte impacto que causaron en el mundo de la tecnología*. Obtenido de http://www.iprofesional.com/notas/122250-Los-ataques-del-11-S-y-el-fuerte-impacto-que-causaron-en-el-mundo-de-la-tecnologia?page_y=0

Ernst & Young. (2017). *Promoviendo el desarrollo de una cultura de prevención - Estudio de gobierno, gestión de riesgos y auditoría interna en el Perú 2016-17*. Obtenido de http://larepublica.pe/economia/868843-ey-peru-el-52-de-las-empresas-peruanas-no-cuenta-con-un-plan-de-contingencia-ante-desastres-naturales

Gestión. (2015). *Para la certificación de ISO, el Perú es un "mercado muy reducido"*. Obtenido de https://gestion.pe/economia/empresas/certificacion-iso-peru-mercado-reducido-93181

Gonzáles et al. (2017). *Últimos cortes de luz duraron 10 veces más que el promedio de las interrupciones de 2016*. Obtenido de http://www2.latercera.com/noticia/ultimos-cortes-luz-duraron-10-veces-mas-promedio-las-interrupciones-2016/

Instituto de Auditores Internos. (2017). *Gestión estratégica del talento en Auditoría Interna*.

Madrid: Desdecero Estudio Gráfico.

ISO. (2010). UNE-ISO: 31000 *Gestión del riesgo. Principios y directrices.*

ISO. (2011). 19011:2011 *Directrices para la auditoría de Sistemas de Gestión*.

ISO. (2015). ISO 22317:2015 *Seguridad social – Sistemas de Gestión de Continuidad de Negocios – Directrices para el análisis del impacto de negocios*.

ISO. (2015). UNE-EN ISO 22301: 2012 *Protección y seguridad de los ciudadanos Sistema de Gestión de la Continuidad del Negocio Especificaciones*. Obtenido de https://gestion.pe/blog/riesgosfinancieros/2014/09/continuidad-operativa-o-del-negocio-ejemplos-de-exito.html

Omendi, M (2003). *EL mundo después de la caída de las torres gemelas*. Obtenido de http://www.imagenradio.com.mx/el-mundo-despues-de-la-caida-de-las-torres-gemelas

Quevedo, J. (2012). *Revisión de modelos de gestión de continuidad del negocio*. Obtenido de http://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/view/5620/4877

Rittinghouse, J. & Ransome, J. (2005). *Business Continuity and Disaster Recover for InfoSec Managers*. United Kingdom: Elsevier Digital Press.

Sharp's, John. (2012). *Moving from BS 25999-2 to ISO 22301. The new international estándar ofr business continuity management systems*. Obtenido de: https://www.bsigroup.com/Documents/iso-22301/resources/BSI-BS25999-to-ISO22301-Transition-UK-EN.pdf

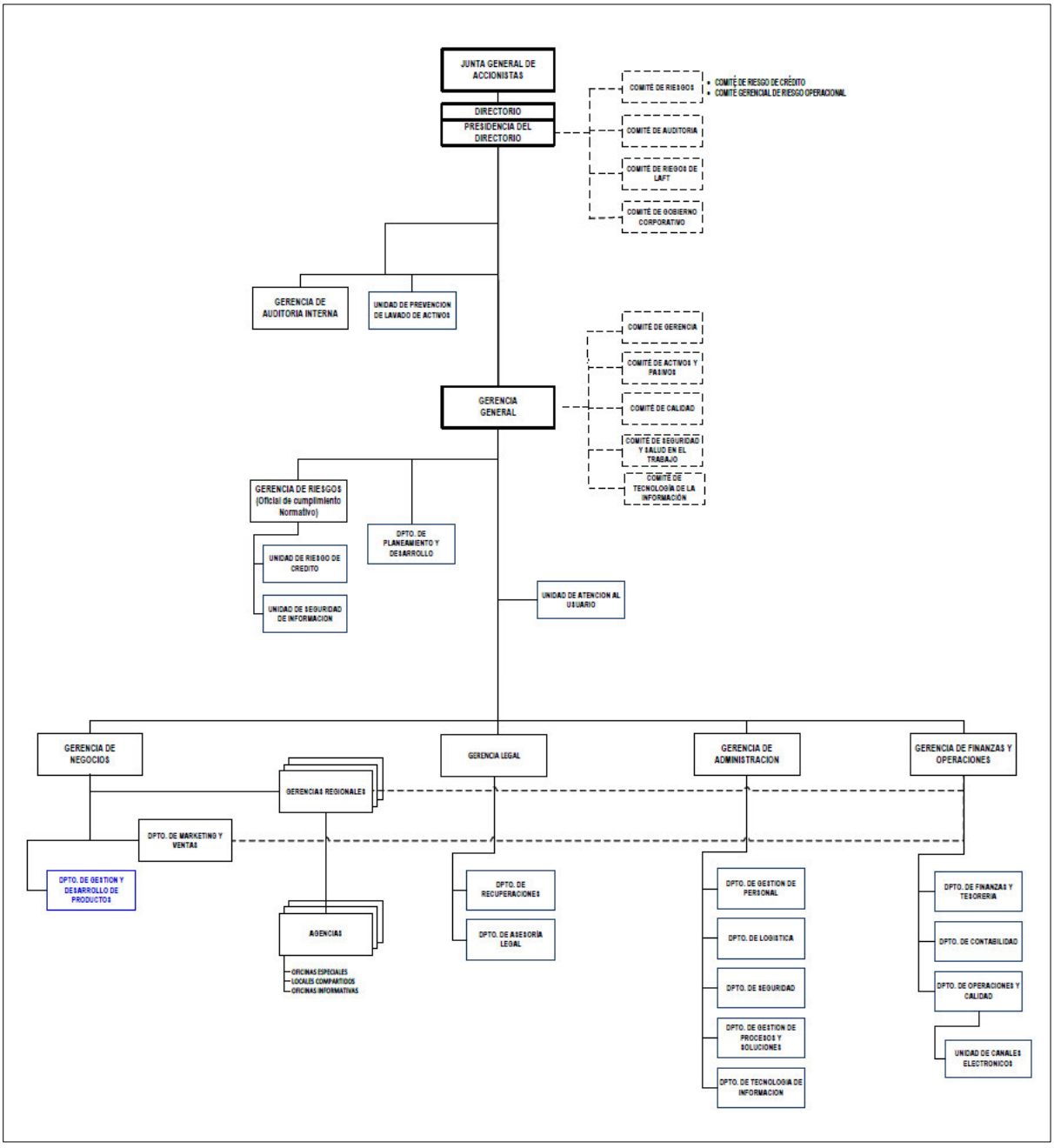
Soto Rodriguez, L. & Céspedes Vargas, K. (2016). *Modelo de un sistema de gestión del negocio para microfinanciera basado en la ISO/IEC 22301 y en la circular G.139-2009 de la SBS*. Lima-Perú: Universidad Peruana de Ciencias Aplicadas (UPC). Obtenido de http://creativecommons.org/licenses/by-nc-nd/4.0/

Yuconza, A. (2018). *Crisis y continuidad del negocio*. Obtenido de http://www.eluniversal.com/noticias/opinion/crisis-continuidad-del-negocio_648725

Zawada, B. (2016). *Implementing ISO 22301. The Business Continuity Management System Standard*. United States of America: Avalution Consulting.

ANEXOS

ANEXO A: Organigrama de la Organización



Fuente: Reglamento de Organización y Funciones de la empresa

ANEXO B: Ubicación de los establecimientos de la entidad financiera

TIPO	UBICACIÓN	REGIÓN
Oficina Informativa	Pampa Cangallo / Putacca	Ayacucho
	Huaccana / Pacucha	Apurimac
Local Compartido	Virú / Chocope	La Libertad
	Canta	Lima
	Mazamari	Junín
	Paucará	Huancavelica
	San Miguel / Querobamba	Ayacucho
	Chuquibamba	Arequipa
Oficina Especial	Huamachuco	La Libertad
	Canto Grande / Jicamarca / José Galvez / Pamplona	Lima
	Huanta / San Franciso	Ayacucho
	Pichari	Cusco
	Uripa	Apurimac
	El Pedregal / Orcopampa / Chivay / Yura	Arequipa
Agencia	Trujillo	La Libertad
	Huanuco / Tingo María	Huánuco
	Ate – Tagore / Carabayllo / Comas / Colonial / Huachipa / Huaycán / Lima Cercado / Los Olivos / Mariscal Cáceres / Manchay / Puente Piedra / San Borja / San Juan de Lurigancho / San Juan de Miraflores / Villa El Salvador / Villa María del Triunfo	Lima
	Huancayo / La Merced / Pichanaki	Junín
	Huancavelica	Huancavelica
	Ayacucho / Puquio	Ayacucho
	Andahuaylas	Apurimac
	Arequipa / Paucarpata	Arequipa

Fuente: Catálogo de agencias del área de Operaciones

ANEXO C: Catálogo de la organización

MACRO PROCESO	PROCESO	SUB PROCESO
Planeamiento y Gestión Estratégicab	Gestión estratégica	Formulación y desarrollo del plan estratégico y operativo
		Seguimiento y control del plan estratégico y operativo
	Desarrollo y administración del presupuesto	Formulación del presupuesto y proyección general de la empresa
		Monitoreo y seguimiento del presupuesto y proyección general
	Gestión de desempeño social	Gestión de internalización de la filosofía institucional
		Gestión e implementación de programas con impacto social y ambiental
		Gestión de indicadores sociales
	Gestión de la información	Elaboración de reportes comerciales y financieros para la toma de decisiones
		Comunicación a los principales stakeholders
Organización y Gobierno Corporativo	Organización	Organización
	Gobierno corporativo	Gobierno corporativo
	Gestión de las relaciones	Gestión de las relaciones
	Gestión de marca	Gestión de marca
Gestión de Cumplimiento	Sistema de prevención de lavado de activos	Elaboración y presentación del plan de trabajo
		Gestión de conocimiento del cliente
		Gestión de conocimiento del mercado
		Gestión de conocimiento del personal
		Capacitación y seguimiento del cumplimiento de la norma
		Presentación del registro de operaciones únicas y múltiples
		Presentación de informes trimestrales y semestrales
	Cumplimiento normativo	Asesoría y capacitación
		Gestión de riesgos de cumplimiento normativo
		Seguimiento, revisión y comunicación
	Gestión de transparencia de información	Elaboración del programa de trabajo
		Monitoreo y control del cumplimiento de las normas de transparencia
		Adecuaciones a las normas de transparencia
		Capacitaciones
		Verificación de los medios de difusión
		Elaboración de informe de gestión
	Auditoría interna	Planificación, determinación del alcance y objetivos
		Identificación y evaluación de controles claves del área auditada
		Validación de funcionalidad de controles claves
		Comunicación de las conclusiones y plan de acción correctivo
		Presentación de informes al directorio y cierre
Gestión por procesos	Gestión de documentos	Elaboración y/o actualización de documentos normativos
		Control y administración de documentos normativos

MACRO PROCESO	PROCESO	SUB PROCESO
	normativos	
	Gestión soluciones	Atención de requerimientos y proyectos
		Gestión y seguimiento de requerimientos y proyectos
	Gestión de mejora de procesos	Seguimiento y gestión de indicadores de procesos
		Gestión de calidad
		Mejora continua de procesos
Gestión de Riesgos	Administración del riesgo	Planificación
		Desarrollo, políticas, estrategias y límites
		Administración de metodologías y modelos
		Gestión de riesgo de capital
	Gestión de riesgo crediticio	Identificación y evaluación de riesgo de crédito
		Mitigación y tratamiento del riesgo de crédito
		Seguimiento y monitoreo
	Gestión de riesgo de mercado y liquidez	Identificación, medición y evaluación del riesgo de mercado y liquidez
		Tratamiento y mitigación del riesgo de mercado y liquidez
		Actividades de control, seguimiento y monitoreo del riesgo de mercado y liquidez
		Evaluación de escenarios de estrés y administración del plan de contingencia de riesgo de mercado y liquidez
	Gestión de riesgo operacional	Identificación, evaluación y tratamiento de riesgos operacionales por procesos
		Evaluación de riesgos por cambios significativos y nuevos productos
		Seguimiento de la gestión de riesgo operacional
		Identificación, comunicación y registro de eventos de pérdida e incidentes
	Gestión de seguridad de la información	Identificación, evaluación y tratamiento de riesgos de los activos de información
		Seguimiento al plan de tratamiento e implementación de controles
		Identificación, comunicación y registro de incidentes y vulnerabilidades
	Gestión de seguridad física y electrónica	Gestión y supervisión de seguridad física y electrónica en agencias y oficinas
		Gestión y prevención de asaltos y fraudes
		Gestión y prevención de accidentes, emergencias y desastres
		Control a la gestión de seguridad física y electrónica
	Gestión de continuidad del negocio	Gestión de continuidad del negocio
	Gestión de prevención del fraude	Análisis e identificación de elementos del fraude
		Control de riesgos del fraude
		Planificación proactiva de detección de fraudes
Mercadeo	Gestión de producto	Investigación de mercadeo
		Evaluación de factibilidad del producto, servicio

MACRO PROCESO	PROCESO	SUB PROCESO
		Diseño o rediseño de producto, servicio, segmento, canal
		Propuesta y aprobación del producto, servicio
		Planificación y diseño de plan de ventas
		Implementación de producto, servicio
		Monitoreo de la implementación de producto, servicio
	Promoción y venta	Promoción y venta directa
		Promoción y venta en canales alternos
Colocaciones	Evaluación	Generación de la solicitud
		Evaluación del crédito
		Gestión de garantía
	Aprobación	Aprobación del crédito
	Desembolso	Contacto y firmas del cliente
		Generación del desembolso
Captaciones de fondos	Fondeo por depósitos del público	Apertura de cuentas
		Depósitos
		Retiros
		Cancelación
		Administración y control de cuentas
	Financiamiento de otras fuentes	Requerimiento de financiamiento
		Gestión del financiamiento
		Cierre de la operación
		Administración y control
Servicios	Venta de servicios	Venta de servicios
	Afiliación de servicios	Afiliación de servicios
Gestión Post-venta	Administración de canales de atención	Administración de efectivo
		Administración del personal de atención al cliente (ventanilla)
		Gestión de transacciones
	Administración de documentos y valorados	Expedición de documentos y valorados
		Digitalización de documentos
		Fiscalización de valorados
		Archivo y custodia de documentos y valorados
	Seguimiento de cartera	Seguimiento de cartera
	Atención al cliente	Atención de consultas
		Atención de solicitudes y reclamos
	Fidelización del cliente	Fidelización del cliente
	Gestión de seguros	Gestión de seguros
Recuperaciones	Recuperación pre judicial	Planificación de la gestión de recuperación
		Contactabilidad del cliente
		Gestión de recuperación del crédito
		Seguimiento y monitoreo

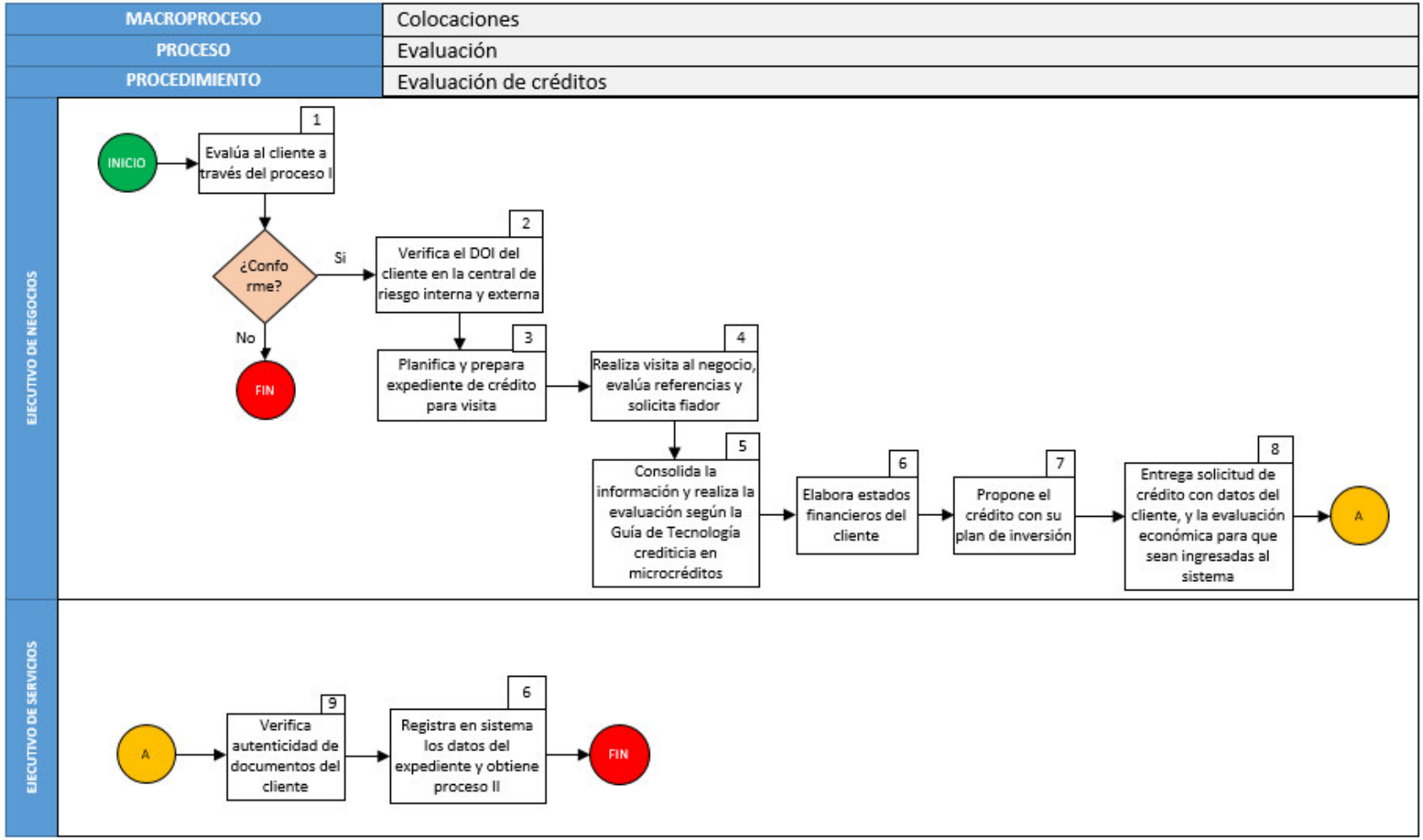
MACRO PROCESO	PROCESO	SUB PROCESO
	Recuperación judicial	Análisis patrimonial del cliente
		Acciones judiciales para clientes sin bienes
		Acciones judiciales para clientes con bienes
		Ejecución de sentencia
		Gestión de gastos judiciales
		Transacción judicial o extrajudicial
	Refinanciamiento y reprogramados	Refinanciamiento
		Reprogramación
	Castigo y venta de cartera	Castigo de créditos
		Recuperación de cartera castigada
		Venta de cartera
Gestión financiera y contable	Administración de liquidez	Proyección de posición de tesorería
		Evaluación de la situación financiera
		Determinación de estrategias de fondeo e inversión
	Inversiones	Análisis de inversión
		Negociación
		Ejecución de la inversión
		Monitoreo
	Administración de tasas y tarifas	Seguimiento continuo de tasas y tarifas
		Elaboración de propuesta de modificación de tasas y tarifas
		Aprobación e implementación de propuesta
	Gestión contable	Registro y validación de movimientos contables
		Gestión de cierre contable
		Análisis de cuentas
		Administración de libros contables
		Gestión tributaria
	Gestión de información financiera y contable	Elaboración y emisión de anexos y reportes para entes regulatorios
Gestión de bienes y servicios	Adquisiciones y contratación de BBSS	Recepción y análisis de requerimiento
		Selección de proveedor
		Contratación de proveedor
		Seguimiento al cumplimiento del contrato
	Atención de útiles y suministros	Recepción de requerimiento
		Aprobación de requerimiento
	Implementación de agencias y oficinas	Aprobación del expediente técnico
		Supervisión de ejecución y entrega de obra
		Arrendamiento y equipamiento de agencia
		Entrega de agencia
	Almacenaje y distribución	Ingreso de bienes
		Transferencia de bienes
		Consumo de bienes
		Control e inventario de almacenes
	Administración	Alta de activo fijo

MACRO PROCESO	PROCESO	SUB PROCESO
	patrimonial	Traslado de activos fijos
		Baja de activos fijos
		Administración de bienes adjudicados
		Mantenimiento (preventivo y correctivo)
		Control de activo fijo
Gestión de recursos humanos	Reclutamiento y contratación	Evaluación y aprobación de puestos
		Reclutamiento y selección de personal
		Administración de contratos
	Desarrollo del colaborador	Capacitación
		Desempeño del colaborador
		Gestión de línea de carrera
	Gestión del colaborador	Vacaciones
		Ceses
		Administración de méritos y deméritos
		Gestión de compensaciones
	Bienestar del colaborador	Bienestar social
		Gestión de subsidios
		Gestión del clima laboral
		Gestión de comunicaciones internas
Asesoría y gestión legal	Gestión de contratos	Gestión de contratos
	Consultoría legal	Consultoría legal
	Gestión de poderes y marca	Gestión de poderes y marca
	Gestión de procesos judiciales	Gestión de procesos judiciales
Gestión tecnológica	Gestión de servicios y atención al usuario	Evaluación y revisión de servicios
		Desarrollo de servicios (incidencias, accesos, información y sistemas)
		Validación de servicio
		Entrega de servicio y soporte
	Gestión de desarrollo de sistema de información	Evaluación de sistema a desarrollar
		Gestión y/o adaptación de sistema de información
		Gestión de calidad
		Gestión de pase a producción
	Gestión de infraestructura, redes y comunicaciones	Monitoreo y mantenimiento de redes y equipos
		Soporte de comunicaciones
		Gestión de backup y disponibilidad de la información
	Administración de base de datos	Gestión de base de datos
		Soporte y mantenimiento de base de datos
		Gestión de seguridad y respaldo de base de datos

Fuente: Catálogo de procesos de la empresa

ANEXO D: Flujograma del proceso de evaluación de clientes

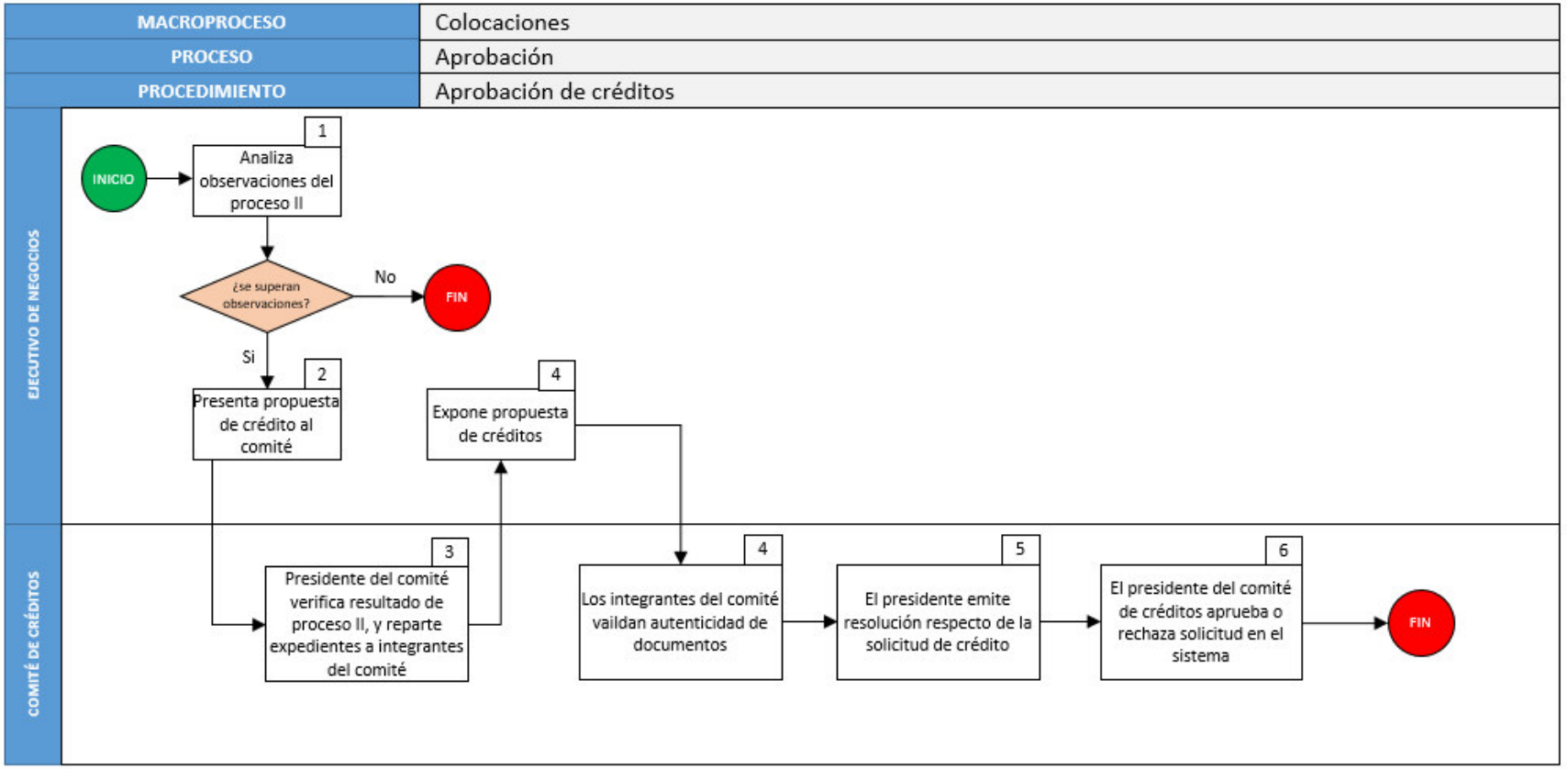
Evaluación de clientes



Fuente: Procedimiento de Promoción, Evaluación y aprobación de créditos

ANEXO E: Flujograma del proceso de aprobación de créditos

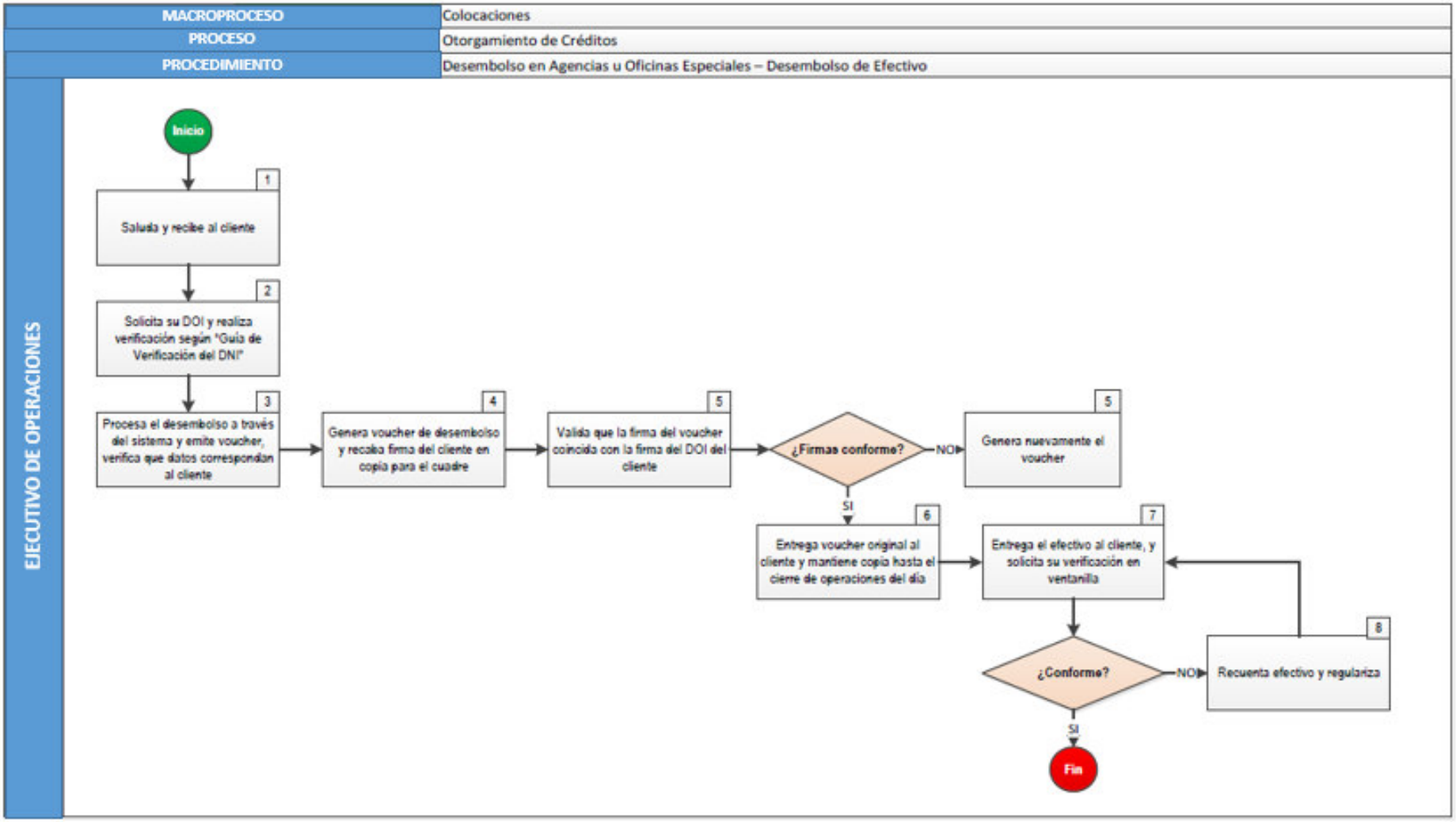
Aprobación de créditos



Fuente: Procedimiento de Promoción, Evaluación y aprobación de créditos

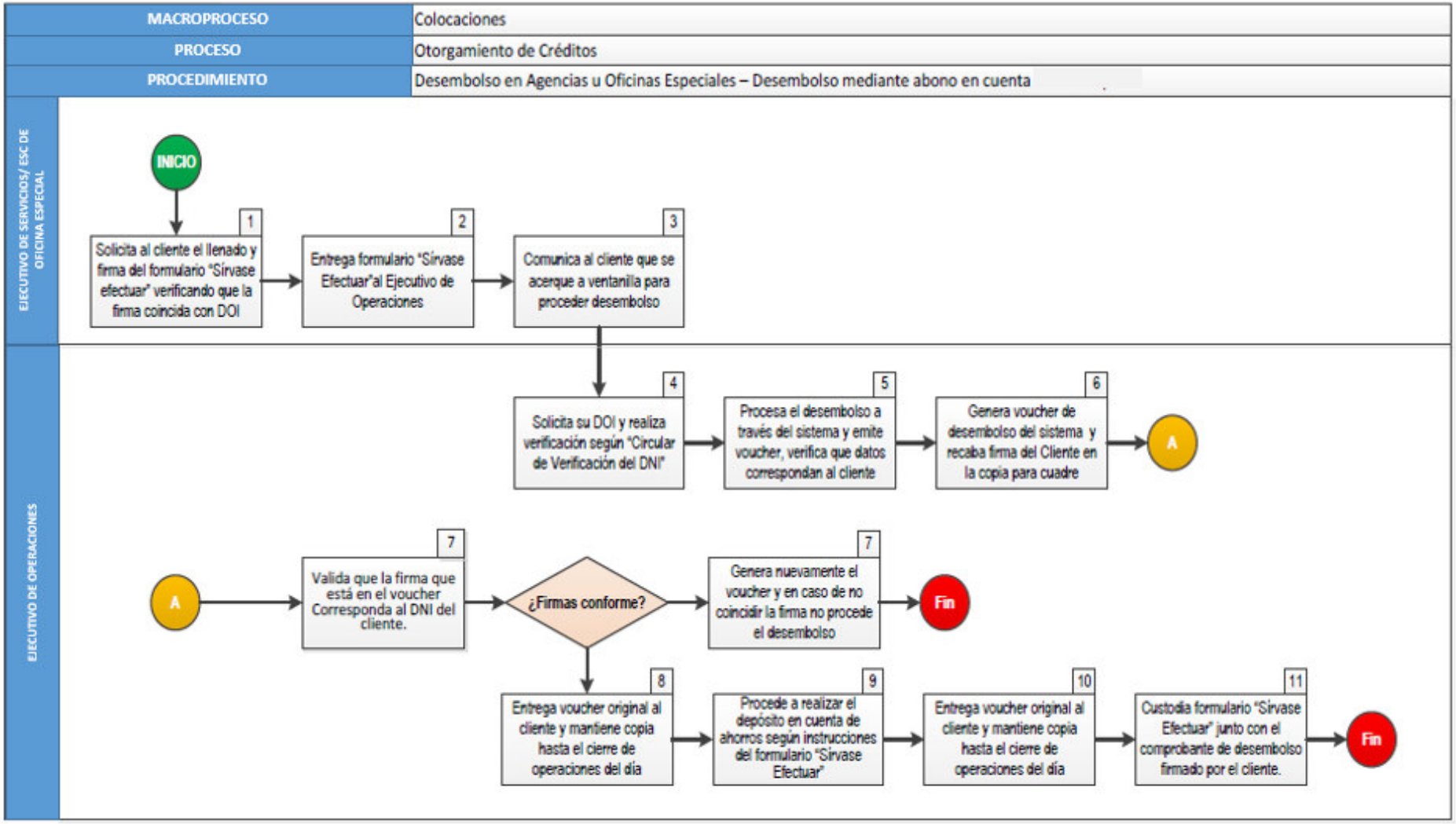
ANEXO F: Flujogramas del proceso de desembolso de créditos

Desembolso en efectivo



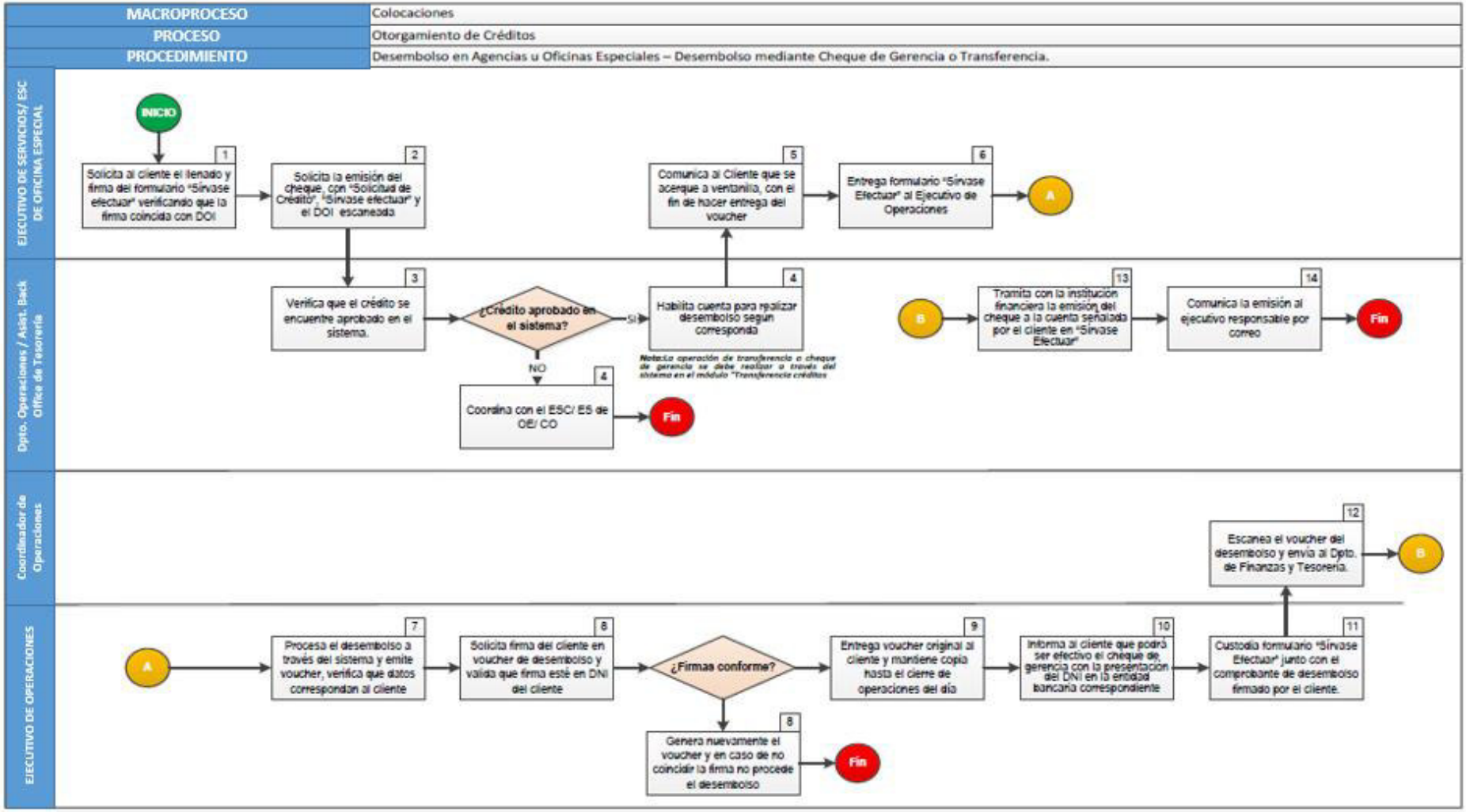
Fuente: Procedimiento de desembolso de créditos

Desembolso mediante abono en cuenta de la empresa



Fuente: Procedimiento de desembolso de créditos

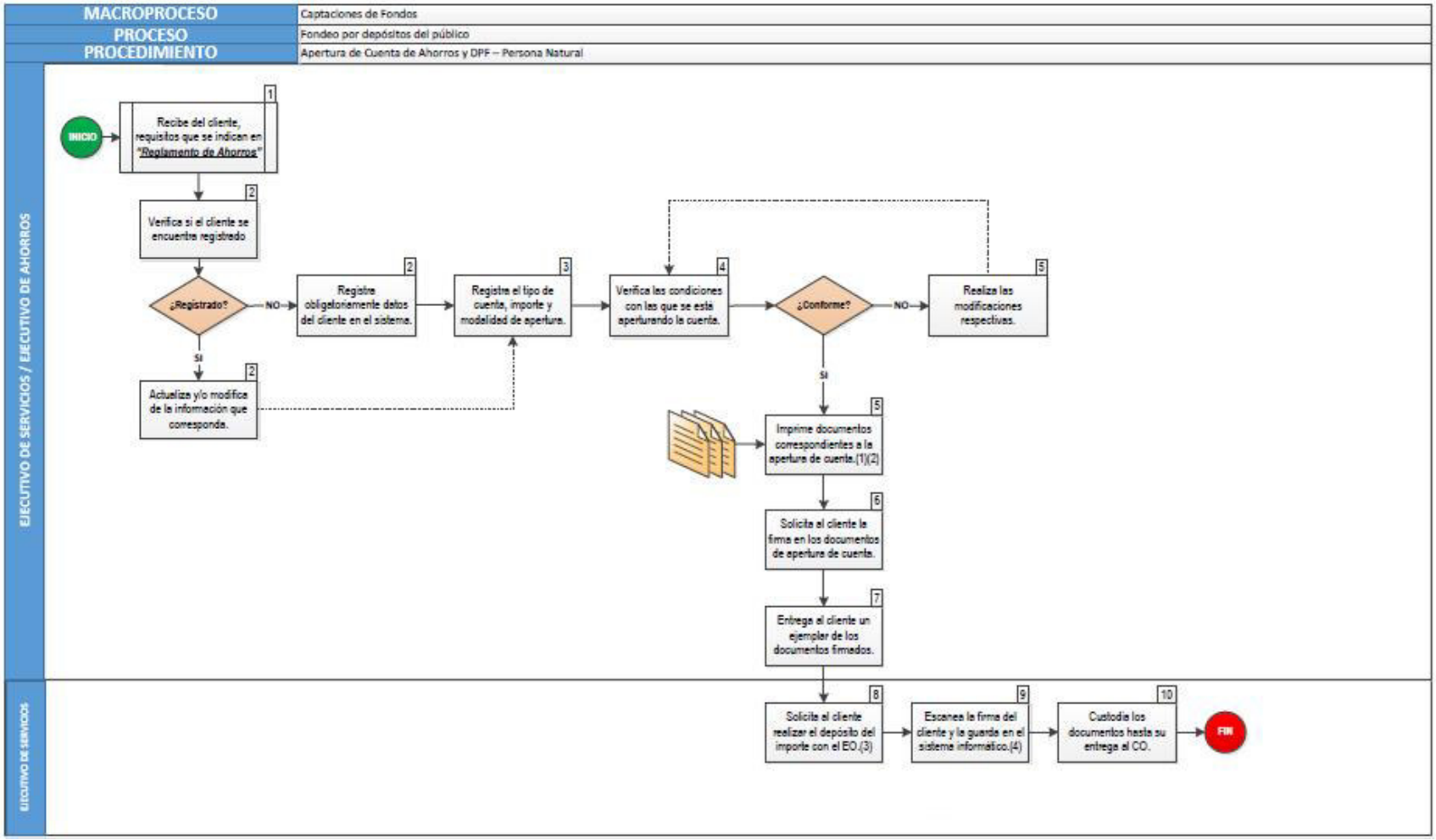
Desembolso mediante cheque de gerencia



Fuente: Procedimiento de desembolso de créditos

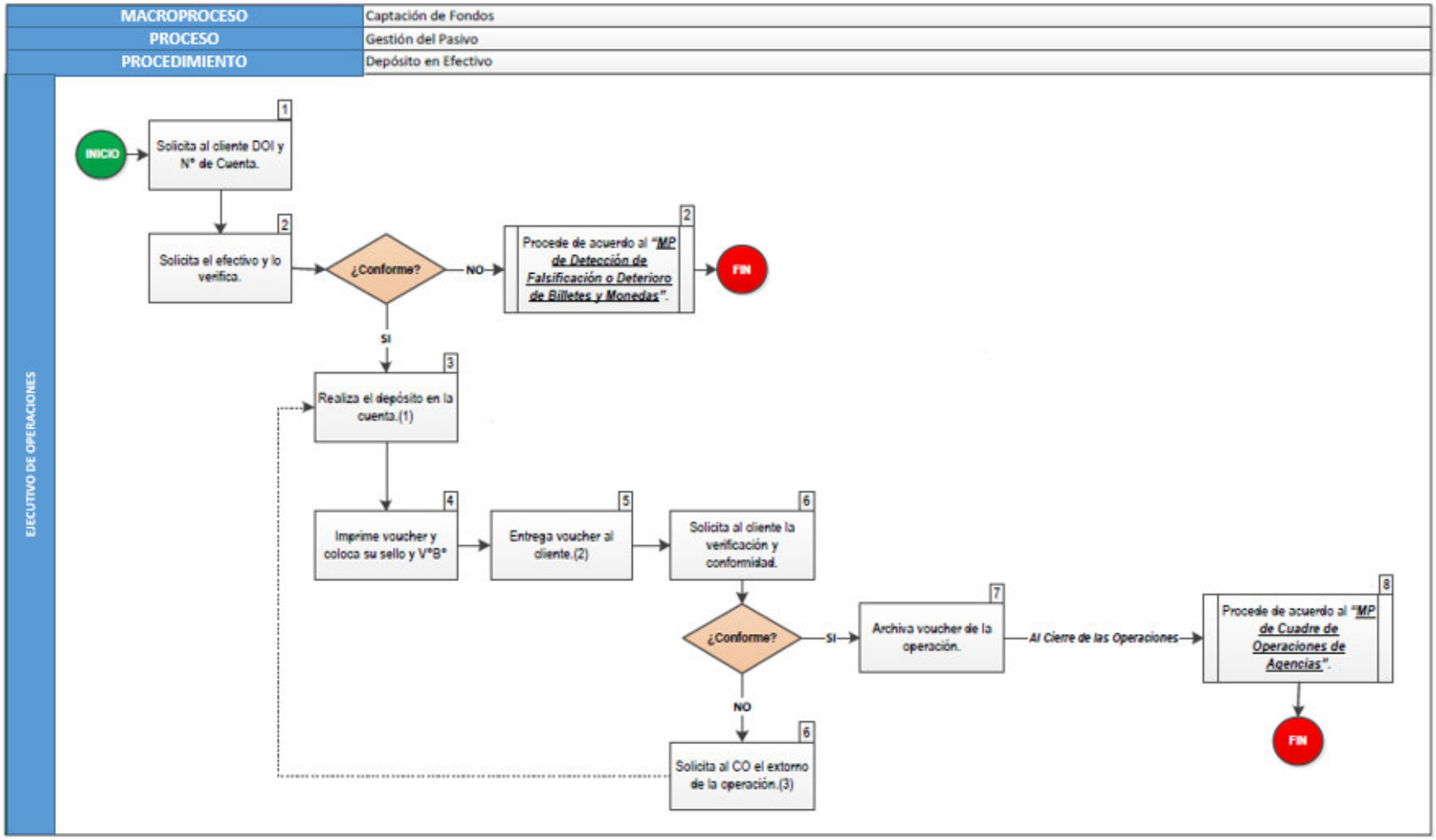
ANEXO G: Flujograma del proceso de fondeo por depósito del público

Procedimiento de apertura de cuenta



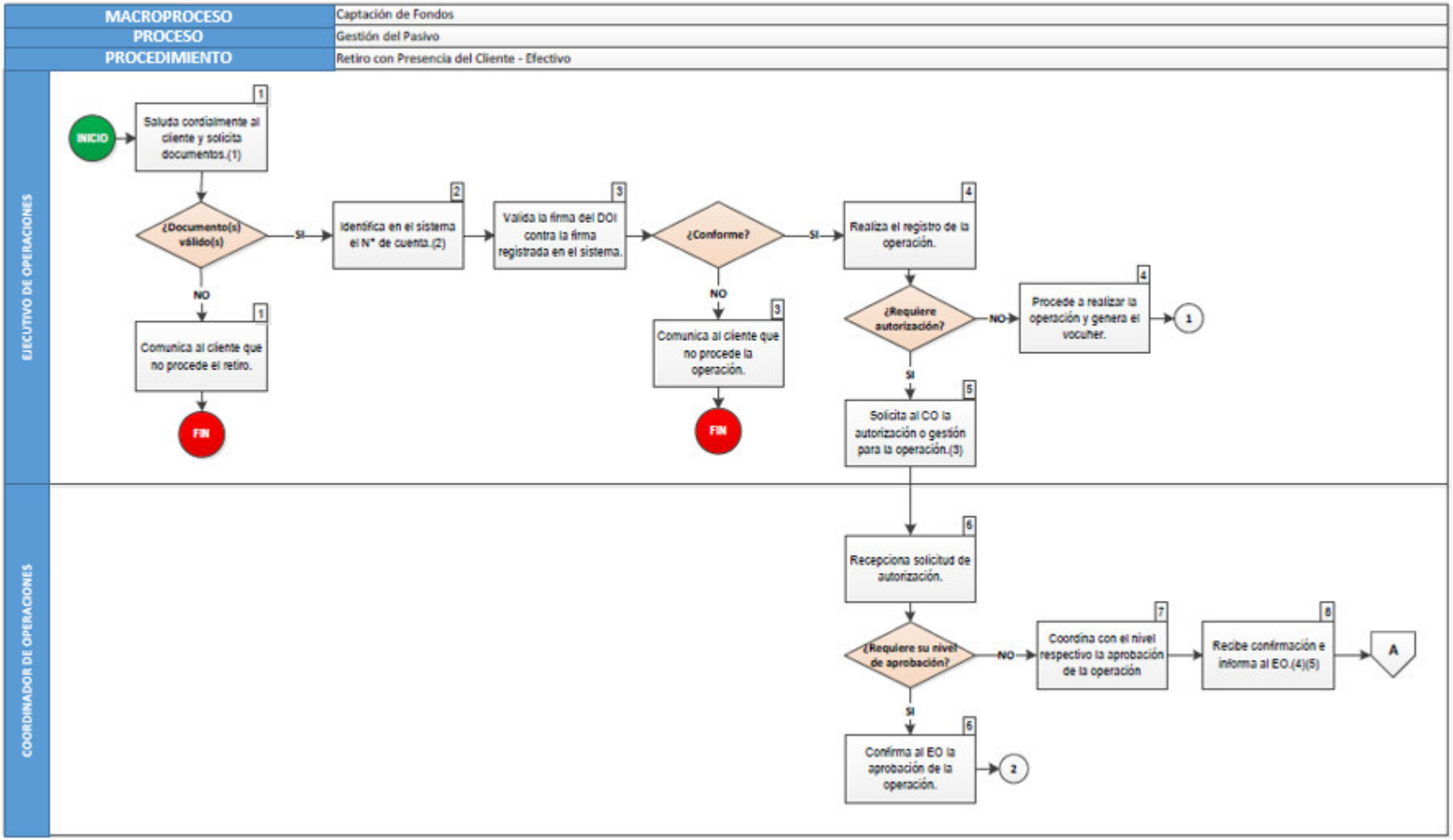
Fuente: Manual de Procedimiento de apertura de cuenta

Procedimiento de depósito



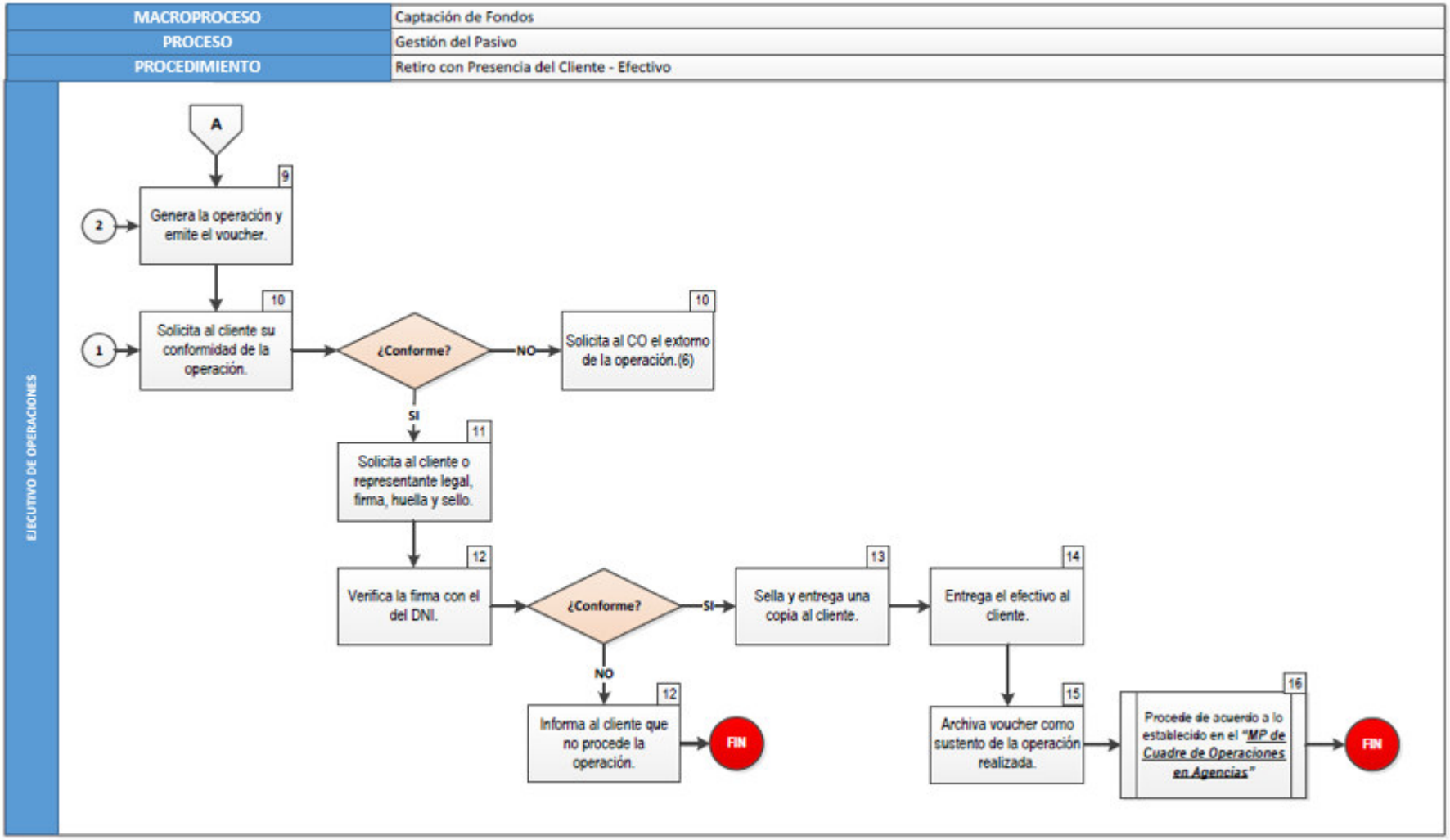
Fuente: Manual de Procedimiento de depósitos

Procedimiento de retiro en efectivo (1)



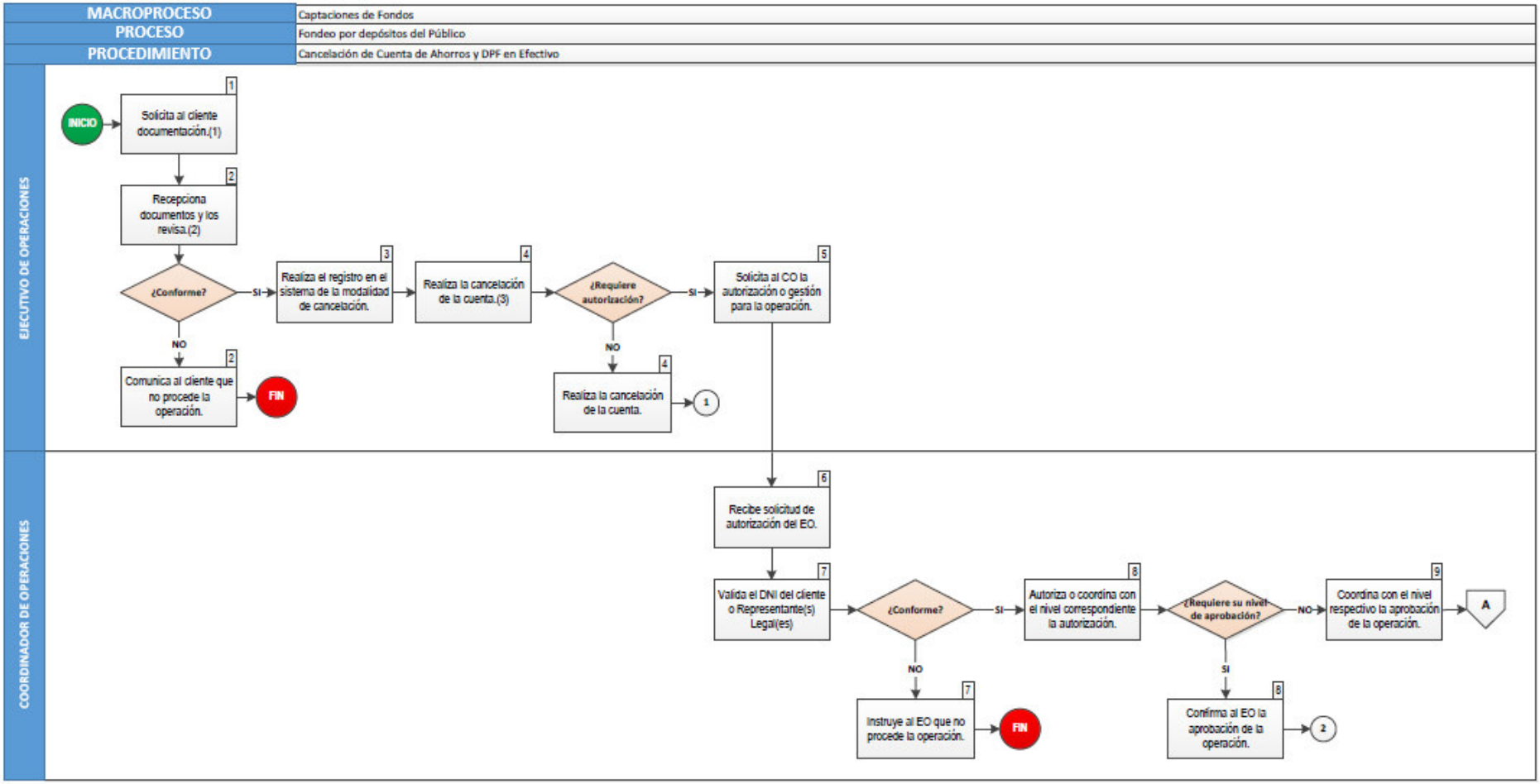
Fuente: Manual de Procedimiento de retiros

Procedimiento de retiro en efectivo (1)



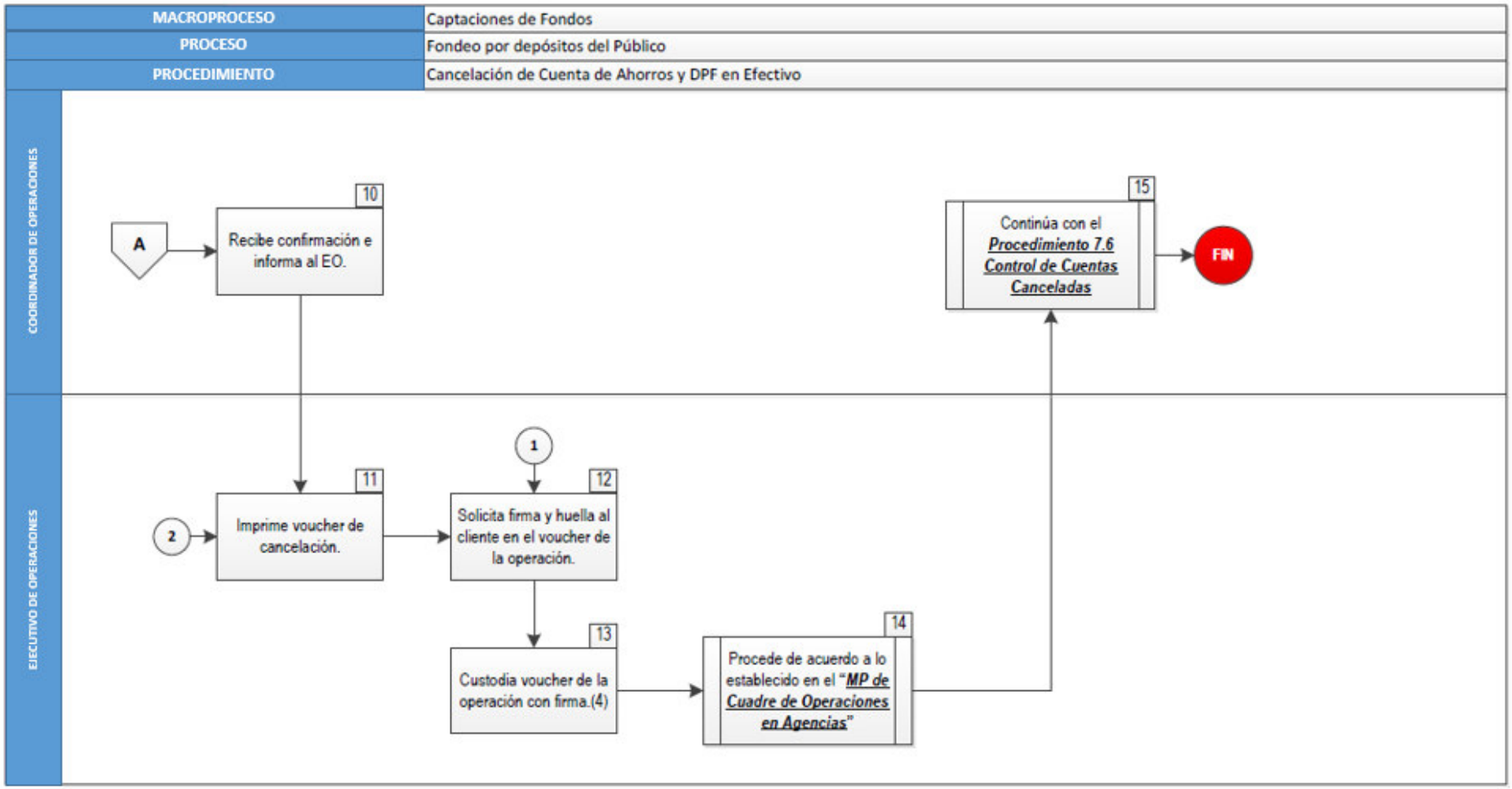
Fuente: Manual de Procedimiento de retiros

Procedimiento de cancelación de cuentas (1)



Fuente: Manual de Procedimiento de cancelación de cuentas

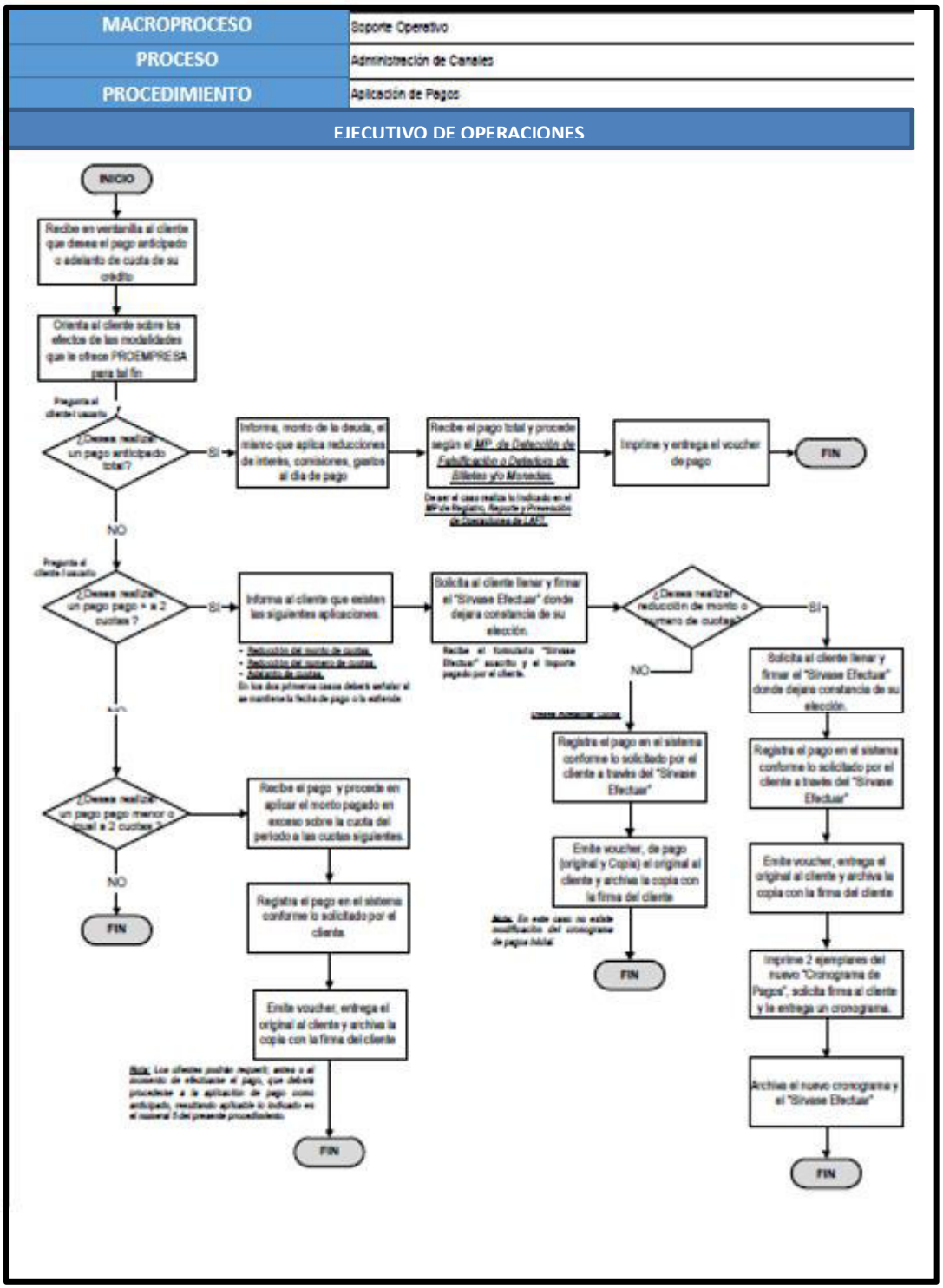
Procedimiento de cancelación de cuentas (2)



Fuente: Manual de Procedimiento de cancelación de cuentas

ANEXO H: Flujograma del proceso de gestión de canales de atención

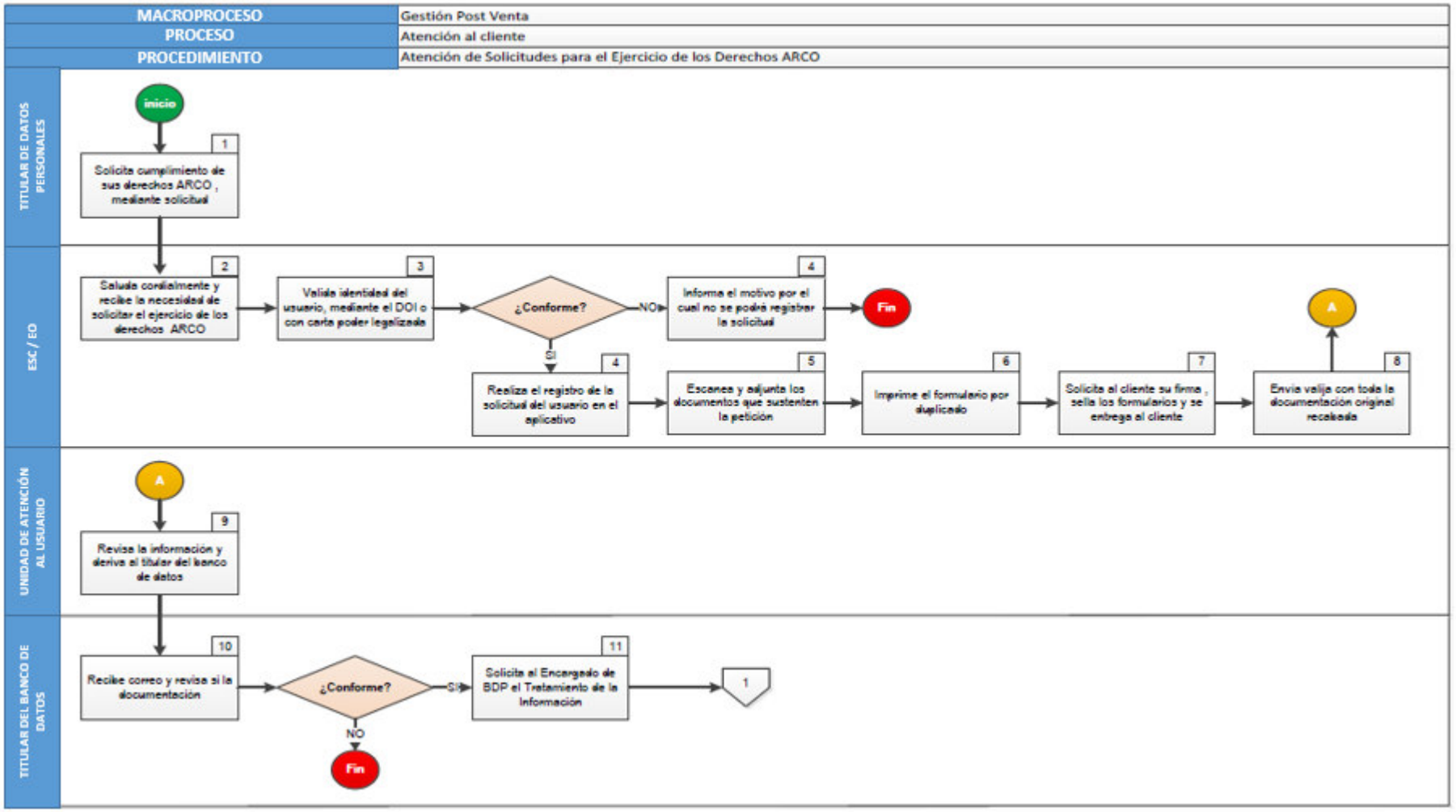
Procedimientos de Pago



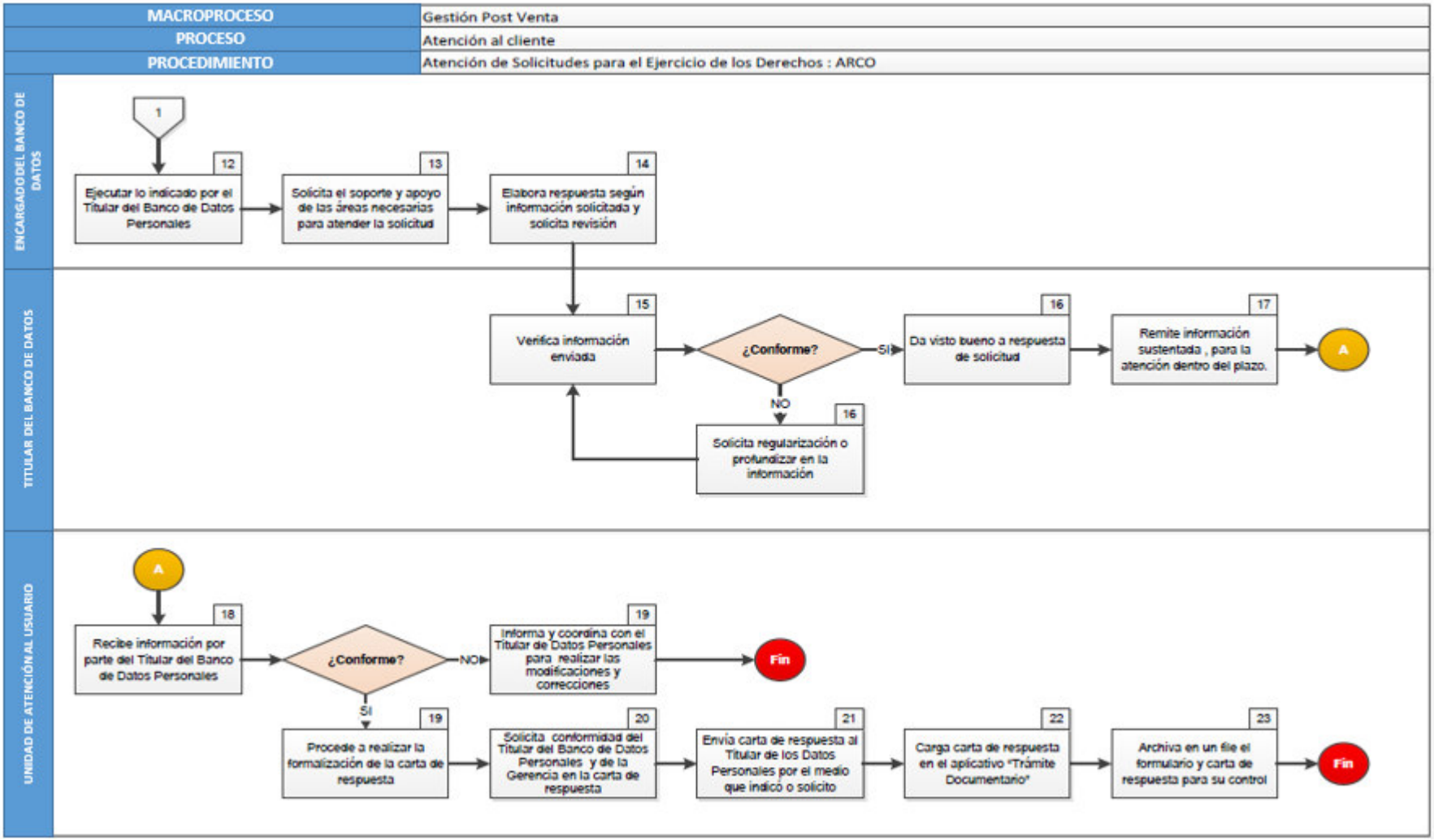
Fuente: Manual de procedimientos de pago adelantado y anticipado

ANEXO I: Flujograma del proceso de atención al cliente

Procedimiento de atención al cliente – Derechos ARCO (1)



Procedimiento de atención al cliente – Derechos ARCO (2)



Fuente: Manual de procedimientos de atención al usuario

ANEXO J: Plan de respuesta de emergencia

1. **Objetivo**:

   Establecer e implementar procedimientos que permita al personal de la organización estar preparados ante situaciones de alto riesgo, tales como desastres naturales o amenazas colectivas que pongan en peligro su integridad física; para lo cual se deben desarrollar acciones rápidas de respuesta.

2. **Alcance**:

   Los aspectos descritos en este plan son aplicables en la oficina principal, así como en las agencias a nivel nacional, en donde la empresa brinda sus servicios.

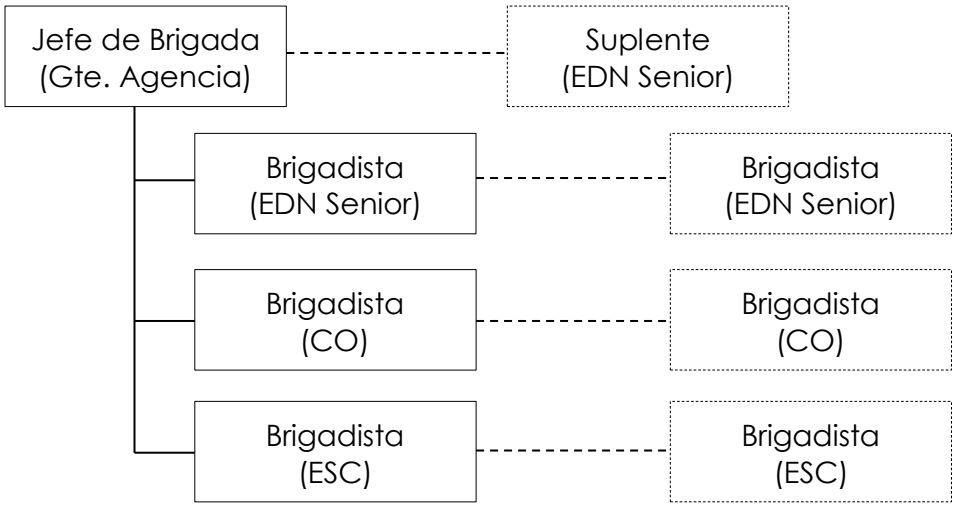
3. **Organigrama de emergencia**:

   Se debe tener en cuenta la siguiente estructura para el despliegue del plan de emergencias.

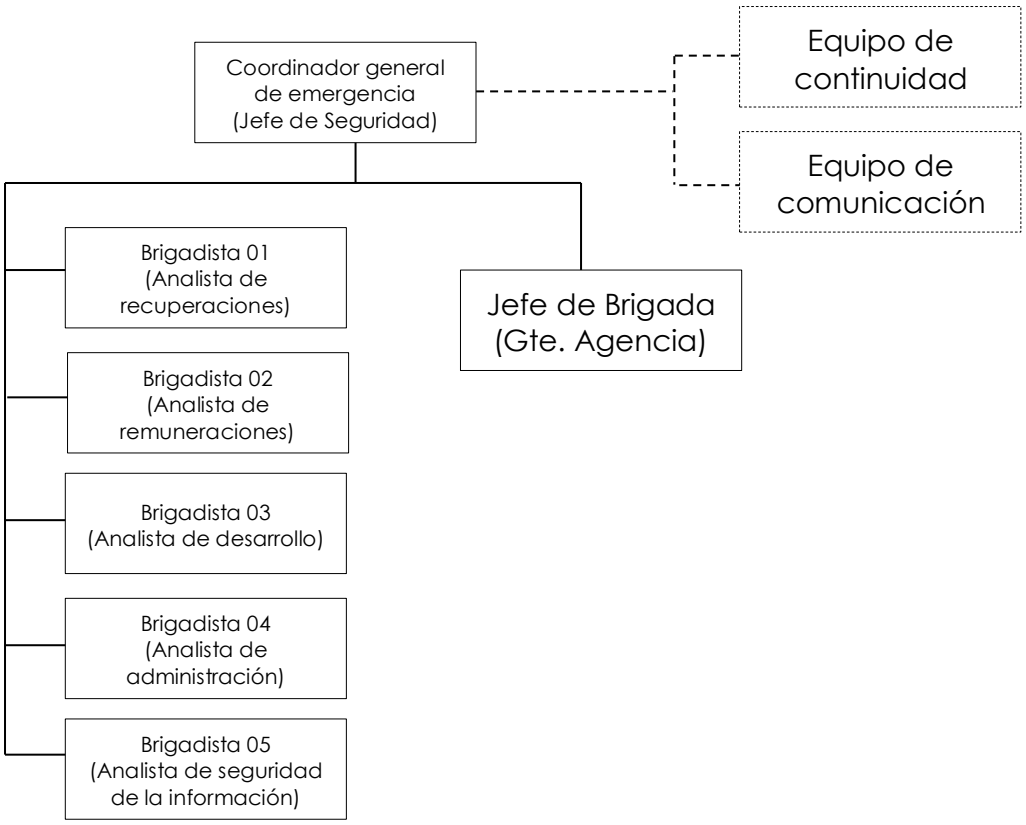
   Los participantes del plan de emergencia son:

Equipo	Integrantes
Personal de alerta	• Todos el personal
Equipo de emergencia en agencia	• Gerente de agencia • Coordinador de operaciones • Ejecutivo de negocios senior • Ejecutivo de servicios
Equipo de emergencia en Oficina Principal	• Jefe de Seguridad • Brigadistas (analista de recuperaciones, analista de remuneraciones, analista de desarrollo, analista de administración, y analista de seguridad de la información)
Equipo de comunicación	• Oficial de desempeño social • Jefe de marketing
Equipo de continuidad del negocio	• Gerente de riesgos • Analista de continuidad

Organigrama de Brigada en agencias:



Organigrama de Brigada en Oficina Principal:



4. Responsabilidades:

- **Coordinador general de emergencia**: Este rol es asumido por el Jefe de Seguridad Física, quien cuenta con las siguientes funciones dentro del comité de emergencia:

  - Responsable de analizar las situaciones de emergencia que se presenten en la organización.
  - Es el responsable directo de coordinar con el equipo de comunicaciones y el

equipo de continuidad a efectos de determinar la activación de planes adicionales.
- Responsable de analizar periódicamente la efectividad del plan de emergencias.
- Responsable de coordinar constantemente con todo el equipo de brigadistas las capacitaciones, el despliegue de simulacros periódicos, la habilitación de rutas de escape, y oportunidades de mejora que puedan presentarse.

- **Jefe de Brigada (Agencia)**: Este rol es asumido por el Gerente de Agencia, o por el Administrador de Oficina Especial, según el tipo de sede (agencia u oficina especial):

  - Responsable de verificar el cumplimiento de capacitaciones y el despliegue de los simulacros en las sedes de agencias.
  - Responsable del despliegue del plan de emergencia en agencias ante situaciones críticas, manteniendo contacto constantemente con el coordinador general de emergencia.
  - Responsable de verificar que los equipos para situaciones de emergencia (extintores, sistema de alarma contra incendio, detectores de humo, y aspersores de agua) se encuentren en correcto estado de funcionamiento.

- **Brigadistas**: Este rol es ejercido, en la oficina principal por un representante de cada piso (desde el segundo hasta el sexto piso); y en agencia por el ejecutivo de negocios senior, el coordinador de operaciones y el ejecutivo de servicios; quienes cuentan con las siguientes funciones:

  - Responsables de guiar y asistir al personal ante situaciones de emergencia.
  - Responsables de capacitar al personal respecto las actividades a ejecutar ante posibles desastres (incendios, terremotos, sismos).
  - Responsables de mantener informados al jefe de brigadas, o al coordinador general de emergencia – según corresponda – respecto al estado en que se encuentra el desastre.
  - Responsables de coordinar la ejecución de las pruebas de forma periódica, así como la emisión de un informe con los resultados obtenidos en cada prueba.

- **Equipo de Comunicación**: Es el equipo encargado de realizar el contacto con el público, con los medios de comunicación y los grupos de interés.

- **Equipo de Continuidad del Negocio**: Es el equipo encargado de analizar la situación indicada por el coordinador general de emergencias, con el objetivo de determinar la convocatoria del comité de crisis.

5. Escenarios de Riesgo

Considerando resultados de la evaluación de riesgos se contemplan para este plan lo siguientes escenarios de interrupción:

Sismos / Terremotos: Evento natural que podría generar pérdidas humanas, monetarias y materiales en la organización.

Asaltos a mano armada: Acto delincuencial no controlado.

Incendio: Se puede entender como la ocurrencia de fuego a grandes dimensiones que

puede generarse de forma fortuita o provocada; y que puede generar pérdidas humanas, monetarias y materiales en la organización.

6. Estrategias – Evento de emergencia sismo

6.1 Estrategias de prevención – Antes de la Emergencia

a. Verificar de forma periódica que las instalaciones cuenten con las señalizaciones y equipos correspondientes, tales como luces de emergencia.
b. Implementar y verificar periódicamente que el botiquín cuente con los implementos necesarios para atender al personal en casos de emergencia.
c. En coordinación con el departamento de seguridad física establecer la ruta de evacuación y los puntos de encuentro del personal.
d. Realizar capacitaciones y concientizar a las brigadas respecto a las funciones que deben desempeñar ante situaciones de emergencia.
e. Realizar simulacros y medir su efectividad.
f. Para aquellas instalaciones que tienen más de 10 años de antigüedad se debe realizar evaluaciones anules y para las demás instalaciones evaluaciones bianuales respecto al estado de la infraestructura de la organización.
g. Las brigadas deberán contar con una relación del personal que se encuentran en las instalaciones.
h. El plan de emergencias deberá ser revisado de forma anual y/o cuando lo disponga el departamento de seguridad.
i. Verificar que los números de contacto de las instituciones que brindan apoyo en casos de emergencia se encuentren actualizados.

6.2 Estrategias de ejecución – Durante la emergencia

a. Activar el plan de emergencias, en el cual las brigadas deberán indicar al personal ponerse a resguardo en las zonas seguras durante el evento.
b. Proceder con la evacuación del personal hacia las zonas seguras establecidas como puntos de reunión.
c. Verificar que todas las personas hayan evacuado las instalaciones.
d. Identificar a las personas que presenten alguna lesión y brindar primeros auxilios.

6.3 Estrategias de cierre – Después de la emergencia

a. En caso de contar con personas que hayan sufrido alguna lesión grave proceder con el traslado de heridos al centro de atención médica más cercano.
b. Analizar con el coordinar general, el inicio del rescate de posibles personas que se encuentren atrapadas en las instalaciones.
c. Analizar con el coordinar general, la conveniencia de retornar a las instalaciones luego de acontecido el evento.
d. Identificar y analizar los daños ocasionados, y posteriormente realizar un informe detallado dirigido al departamento de seguridad física y a la Gerencia General.

7. Estrategias – Evento de emergencia incendio

7.1 Estrategias de prevención – Antes de la Emergencia

a. Verificar periódicamente que las instalaciones cuenten con las señales de seguridad en lugares visibles, y las alarmas en correcto estado.
b. Implementar y verificar periódicamente que los extintores se encuentren ubicados en las zonas correspondientes.
c. Programar revisiones periódicas y verificar la fecha de vigencia de los extintores, a efectos de coordinar la recarga de éstos de forma oportuna.
d. Programar y realizar capacitaciones al personal indicando las áreas seguras y explicando el uso adecuado de los extintores.
e. Realizar revisiones periódicas sobre el estado de las instalaciones eléctricas.
f. Verificar que no existan demasiados aparatos conectados a un mismo tomacorriente, a fin de evitar sobrecargas eléctricas y sobrecalentamiento de los equipos.
g. Verificar que los números de contacto de las instituciones que brindan apoyo en casos de emergencia se encuentren actualizados.
h. Implementar y verificar periódicamente que el botiquín cuente con los implementos necesarios para atender al personal en casos de emergencia.

7.2 Estrategias de ejecución – Durante la emergencia

a. Comunicar a los integrantes de la brigada de emergencias.
b. En caso corresponda comunicarse con la compañía de bomberos.
c. Evitar abrir puertas y ventanas en razón que el aire puede extender el fuego.
d. Las brigadas deberán orientar al personal para que realice la evacuación correspondiente.
e. El personal deberá desplazarse por el suelo, evitando las llamas y el humo en el aire, procurando taparse la boca y la nariz.
f. El personal deberá evitar tocar a las personas afectadas por la corriente eléctrica.
g. Verificar que todas las personas hayan evacuado las instalaciones.

7.3 Estrategias de cierre – Después de la emergencia

a. En caso de contar con personas que hayan sufrido alguna lesión grave proceder con el traslado de heridos al centro de atención médica más cercano.
b. Analizar con el coordinar general, el inicio del rescate de posibles personas que se encuentren atrapadas en las instalaciones.
c. Identificar y analizar los daños ocasionados, y posteriormente realizar un informe detallado dirigido al departamento de seguridad física y a la Gerencia General.

8. Estrategias – Evento de emergencia asalto

8.1 Estrategias de prevención – Antes de la Emergencia

a. Revisar de forma periódica que los controles y medidas de seguridad se encuentren en funcionamiento.
b. Contar con procedimientos para el arqueo de efectivo en bóveda cuando la agencia se encuentra cerrada.
c. Se establecerán cámaras en zonas estratégicas, cajas, antebóveda y bóveda.
d. Realizar pruebas periódicas al sistema de alarmas a fin de verificar su adecuado funcionamiento.
e. Realizar las operaciones de remesas (envío y recepción de efectivo) en horarios no rutinarios.

f. Capacitar al personal de agencias a efectos que tomen conocimiento del funcionamiento de los sistemas de alarma.

8.2 Estrategias de ejecución – Durante la emergencia

a. Toda acción por parte del personal debe estar orientada a proteger y salvaguardar la vida e integridad física.
b. El personal deberá mantener la calma y no realizar actos imprudentes que puedan poner en peligro la vida o integridad de las personas que se encuentran en las instalaciones.
c. El personal debe acatar las órdenes de los delincuentes, considerando que la alarma solo debe activarse cuando éstos se encuentren fuera de las instalaciones.

8.3 Estrategias de cierre – Después de la emergencia

a. Se procederá con el cierre de las instalaciones y se esperará por el arribo de las autoridades.
b. Comunicar el evento ocurrido al equipo de contingencia.
c. Elaborar un informe de lo sucedido y proceder con la gestión de los seguros correspondientes.

9. Retorno a la normalidad

Finalmente, cuando el evento adverso haya culminado, el plan de emergencia debe desactivarse; debido a ello es necesario contar con un procedimiento para el retorno a las actividades, considerando que en caso no se puede retornar a las operaciones tal y como se encontraban antes del incidente, deben considerarse niveles mínimos aceptables de operación, los cuales pueden incluir procedimientos manuales.

Consideraciones a tener en cuenta luego de un sismo/terremoto e incendio para el retorno al trabajo:

- Colaborar con las autoridades verificando la seguridad del área afectada.
- Coordinar con el personal para que no ingrese a las zonas afectadas mientras las autoridades no lo dispongan.
- Coordinar con el personal a efectos que se mantengan en zonas seguras debido a posibles réplicas.
- Coordinar con las autoridades, y esperar por la conformidad indicando que la infraestructura no ha sufrido daños considerables y que puede ser habitable. Considerar que esta conformidad no necesariamente será otorgada el mismo día.
- Proceder con el reinicio de las labores en las sedes correspondientes, para lo cual deberán considerar los planes de recuperación del negocio.

Consideraciones a tener en cuenta luego de un asalto para el retorno al trabajo:

- Posterior al evento deben cerrarse las instalaciones, y se esperará por el arribo de las autoridades.
- Colaborar con las autoridades describiendo el evento acontecido.
- Coordinar con las autoridades la apertura de las instalaciones a efectos de volver a operar nuevamente.

10. Teléfonos de Emergencia – Rol de llamadas

En esta sección se describe la institución y el número telefónico de contacto. Al respecto se debe tener en cuenta que este listado deber ser actualizado periódicamente.

- Cuerpo General de Bomberos Voluntarios del Perú
- Central de emergencias
- Comisaría del sector
- Municipalidad del distrito
- Empresa que brinda servicios de electricidad
- Hospital de emergencia de la localidad o provincia
- Proveedores de servicios de agua y gasfitería
- Proveedor de grupo electrógeno

11. Lista de equipos (extintores)

En esta sección deben indicarse la cantidad de extintores que se tienen y la ubicación de los mismos.

- Extintores de tipo CO2
- Extintores PQS

12. Organización de brigadas

En esta sección se debe indicar el nombre de las personas que forman parte de las brigadas de emergencia. Se debe tener en cuenta que esta sección debe ser actualizada constantemente, debido a la rotación de personal.

a. Jefe de Brigada
   Titular: …… Teléfono: ……..
   Suplente: ……. Teléfono: ……..

b. Brigadista
   Titular: …… Teléfono: ……..
   Suplente: ……. Teléfono: ……..

c. Brigadista
   Titular: …… Teléfono: ……..
   Suplente: ……. Teléfono: ……..

d. Brigadista
   Titular: …… Teléfono:

……..
Suplente: ……. Teléfono:
……..

13. Plano de evacuación

En esta sección se debe adjuntar el plano de distribución de las instalaciones y deberá ubicarse dentro del panel o mural visible para el personal.

ANEXO K: Plan de gestión de crisis

1. **Objetivo**:

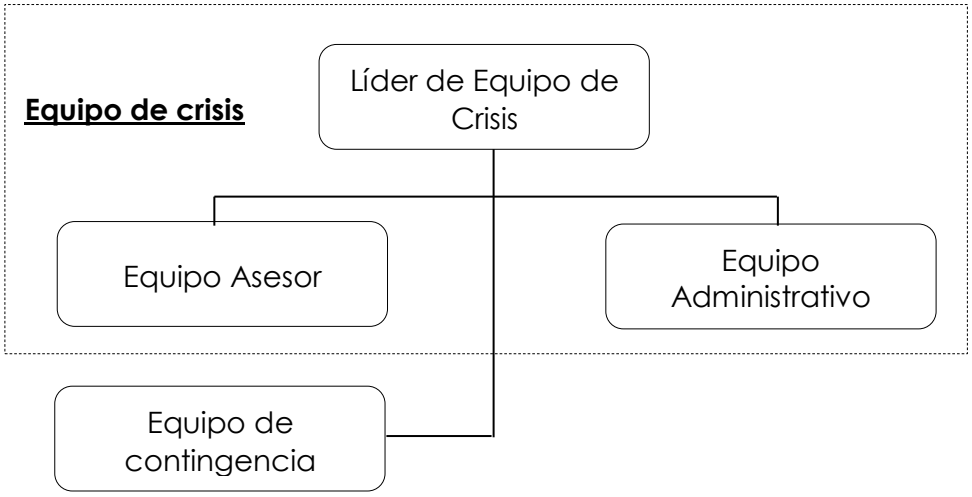
   El plan de gestión de crisis tiene por objetivo establecer una serie de procedimientos que permitan hacer frente a la fase más crítica o aguda de un evento disruptivo que ponga en alto riesgo a la organización. Para ello deberán establecer criterios de activación del plan, los roles y las responsabilidades que tiene el personal para ejecutar estos procedimientos, así como los criterios de desactivación y retorno a las operaciones.

2. **Alcance**:

   El manual de gestión de crisis es aplicable en toda la organización, en caso suceda un evento de crisis que afecten las operaciones en la oficina principal como en las agencias.

3. **Roles y responsabilidades**:

   Para el despliegue de este plan se debe de establecer y formalizar la conformación de un comité de crisis.
   Este comité debe estar capacitado para poder brindar una respuesta oportuna ante una situación de crisis. Asimismo, será responsable de ejecutar procedimientos administrativos, de comunicación y coordinación a todo nivel. Este equipo estará conformado de la siguiente forma:



- **Líder de equipo de crisis**: Es el responsable de liderar la ejecución de actividades del equipo asesor, el equipo administrativo y de la comunicación constante con el equipo de contingencia. Por otra parte, es responsable también de liderar el plan de comunicación.

- **Equipo asesor**: Equipo encargado de brindar orientación sobre las estrategias y procedimientos a ejecutar.

- **Equipo administrativo**: Este equipo tiene por responsabilidad desarrollar estrategias alternas a las que ya se encuentran definidas.

- **Equipo de contingencia**: Este equipo es el responsable de dar inicio a las acciones definidas por el comité de crisis.

Integrantes del equipo de crisis:

Rol	Integrantes	Suplentes
Líder de equipo de crisis	• Gerente General	• Director
Equipo asesor	• Gerente de Riesgos • Analista senior de continuidad del negocio	• Oficial de Seguridad de la Información • Analista senior de riesgo operacional
Equipo Administrativo	• Gerente de Finanzas • Gerente de Negocios • Gerente de Administración	• Jefe de Finanzas y Tesorería • Gerente Regional • Jefe de TI
Equipo de contingencia	• Jefe de Operaciones (líder) • Jefe de Finanzas y Tesorería • Jefe de Gestión de Personal • Jefe de TI • Jefe de seguridad • Jefe de Logística • Oficial de seguridad de la información • Gerente de agencia • Coordinador de operaciones	• Analista de operaciones • Analista de finanzas • Asistente de compensaciones • Analista Senior de Producción • Asistente de seguridad • Analista de logística • Analista de riesgo operacional • Coordinador de agencia • Ejecutivo de servicios

Entiéndase que una situación de crisis, es la fase más aguda de un evento que genera afectación a diversos procesos en la organización, y debido a ello, conjuntamente con el plan de gestión de crisis se genera la activación de diversos planes de recuperación de negocios.
Entre las principales responsabilidades de los miembros del comité de crisis, se encuentran las siguientes:

- **Líder de equipo de crisis – Gerente General (Director – Suplente):**
  - Convocar y dirigir los comités de crisis.
  - Tomar decisiones que permitan dirigir el proceso de recuperación del negocio, ante escenarios de interrupción.
  - Establecer y mantener los canales de comunicación con los diversos grupos de interés.
  - Convocar al equipo de continuidad para el análisis de la situación.

- **Equipo asesor - Gerente de riesgos (OSI – Suplente):**
  - Asesorar al líder del equipo de crisis respecto a la toma de decisiones en representación del Directorio.
  - Supervisar al equipo de contingencia en la aplicación de estrategas y procedimientos de recuperación del negocio.

- **Equipo asesor – Analista senior de continuidad del negocio (analista de riesgo**

operacional – suplente):

- Asesorar al líder del equipo respecto a la aplicación de estrategias y procedimientos de recuperación del negocio.
- Difundir periódicamente el plan de gestión de crisis, y verificar que el personal se encuentre capacitado para su despliegue ante situaciones críticas.

- **Equipo administrativo – Gerente de Finanzas (Jefe de finanzas y tesorería - suplente):**
  - Dirigir las actividades de recuperación del proceso de gestión financiera.
  - Velar por el cumplimiento de los tiempos de recuperación en el proceso de finanzas y ahorros.
  - Monitorear y comunicar de forma permanente la liquidez de la empresa.

- **Equipo administrativo – Gerente de Negocios (Gerente regional – suplente):**
  - Dirigir las actividades de recuperación del proceso de créditos.
  - Velar por el cumplimiento de los tiempos de recuperación en el proceso de créditos.

- **Equipo administrativo – Gerente de Administración (Jefe de TI – suplente):**
  - Verificar que la organización cuente con los recursos necesarios para los procesos de recuperación de acuerdo con los planes y procedimientos establecidos.
  - Velar por la atención del personal con daños físicos en situaciones de emergencia. Deberá estar en contacto permanente con el coordinador general de emergencias (plan de emergencia).

- **Equipo de contingencia – Jefe de Operaciones (Analista de operaciones – suplente):**
  - Supervisar los procedimientos de contingencia en agencias.
  - Dar inicio operativo al manual de continuidad de agencias.
  - Velar por la ejecución de procedimientos durante la crisis de forma que no se genere interrupción en los procesos de atención al cliente.
  - Informar al equipo administrativo de los incidentes o situaciones no críticas que se han presentado en la institución.
  - Verificar que luego de culminado el evento de crisis se ingrese la información recabada de forma manual en los sistemas que corresponda.
  - Requerir constantemente información sobre el estado de las agencias durante el evento de crisis.

- **Equipo de contingencia – Jefe de Finanzas y Tesorería (Analista de finanzas - suplente)**
  - Mantener actualizados los archivos de gestión de liquidez y presentar los reportes a la Gerencia de Finanzas.
  - Verificar el importe del efectivo en cada una de las agencias a fin de monitorear la liquidez de las mismas.
  - Monitorear la liquidez de la empresa con mayor detalle durante el evento de crisis.

- **Equipo de contingencia – Jefe de Gestión de Personal (Asistente de compensaciones - suplente)**
  - Apoyar a los líderes de los equipos para convocar y al personal involucrado en el plan de gestión de crisis.
  - Verificar que los heridos luego de algún evento de emergencia reciban la atención médica correspondiente.

- Liderar procedimientos contingentes a efectos que el retraso en pagos del personal no agrave el evento de crisis.
- Mantener actualizado el listado de contactos de emergencia del personal.

- **Equipo de contingencia – Jefe de TI (Analista senior de producción - suplente)**
  - Velar por el cumplimiento de los tiempos de recuperación en los servicios que brinda el departamento de TI.
  - Comunicar permanentemente a la Gerencia de Riesgos y a la Jefatura de Operaciones las interrupciones de los servicios de TI en las situaciones en que no se cuente con tiempo estimado de recuperación; y posteriormente informar cada cuatro horas, la situación de dichos servicios.
  - Liderar la ejecución del plan de recuperación de desastres de TI (DRP)
  - Realizar evaluaciones periódicas del estado de la infraestructura tecnológica de la organización.
  - Custodiar durante la crisis los activos tecnológicos que le han sido asignados.

- **Equipo de contingencia – Jefe de seguridad (Asistente de seguridad - suplente)**
  - Proponer al equipo de crisis las medidas de seguridad que se deben implementar con el objetivo de salvaguardar los activos de la empresa.

- **Equipo de contingencia – Jefe de logística (Analista de logística - suplente)**
  - Coordinar con la Gerencia de Administración para abastecer de equipos e insumos para el despliegue de los procedimientos de contingencia.
  - Verificar el cumplimiento de los tiempos establecidos para la distribución e instalación de equipos necesarios para hacer frente al evento de crisis.
  - Mantener actualizado el listado de proveedores para atender situaciones de emergencia y crisis.

- **Equipo de contingencia – Oficial de seguridad de la información (Analista de riesgo operacional - suplente)**
  - Verificar por el resguardo de la información sensible que gestiona la organización.
  - Analizar posible pérdida de información crítica de la empresa, y coordinar constantemente con el departamento de TI la ejecución de procedimientos de respuesta.

- **Equipo de contingencia – Gerente de agencia (Coordinador de agencia - suplente)**
  - Reportar a la Gerencia Regional y a la Gerencia de Negocios eventos que atenten contra la continuidad del negocio y que puedan conllevar a una situación de crisis.
  - Verificar el cumplimiento de la ejecución de planes de continuidad.
  - Desarrollar las actividades en agencia designadas por el líder del equipo de crisis.

- **Equipo de contingencia – Coordinador de operaciones (Ejecutivo de servicios - suplente)**
  - Dirigir a los ejecutivos de operaciones para proceder con la ejecución de procedimientos manuales.
  - Atender los procedimientos orientados a identificar el nivel de liquidez de la agencia, y mantener informado al Jefe de Tesorería.
  - Verificar la ejecución de estrategias comunicadas por el comité de crisis a efecto de evitar riesgos reputacionales.

El equipo administrativo y el equipo de continuidad del negocio serán los responsables de revisar y actualizar de forma periódica el plan de gestión de crisis, considerando los siguientes aspectos:

- El plan de gestión de crisis será actualizado de forma anual, o en caso se presente la implementación de una nueva línea de negocio, o cambios en la dirección de estrategias del negocio.

4. Criterios de activación

Para la activación del plan de crisis se considera la ocurrencia de eventos que conlleven a un impacto grave en la organización, entre los cuales – sin ser limitante – se encuentran los siguientes:

FACTOR	TIPO DE AMENAZA	AMENAZA
Eventos externos	Desastres	Terremoto
		Incendios
	Interrupción de servicios públicos	Caída del servicio de internet
		Corte de suministros de energía eléctrica
	Actos delictivos	Atentados a las oficinas
		Robo en la sala de servidores
Personas	Sabotaje	Sabotaje interno a los servicios o recursos de TI
	Ausencia de trabajadores clave	Faltas, enfermedades
TI	Falla de sistemas internos	Falla en sistema eléctrico interno
		Fallas en cableado de red
	Falla en servidores	Fallas en servidores principales
	Falla en comunicaciones	Fallas en equipos de comunicaciones
	Falla en software core	Corrupción del software del CORE del negocio

5. Plan de Acción

5.1 Fase Antes – Actividades de preparación

a. Verificar que el plan de gestión de crisis se encuentre disponible y actualizado.
b. Verificar que los miembros del comité de crisis sean capacitados periódicamente en sus funciones.
c. Verificar que se cuente con los recursos disponibles para el despliegue de las acciones establecidas en el plan de gestión de crisis.
d. Asegurar el resguardo de registros vitales.
e. Asegurar que los proveedores críticos cuenten con planes de continuidad para hacer frente a situaciones que afecten sus operaciones relacionadas con la organización.
f. Programar pruebas anuales respecto a la ejecución de los planes de crisis.

g. Concientizar a los miembros del comité respecto a los riesgos que enfrente la organización.

5.2 Fase Durante – Actividades de respuesta y de operación alterna

a. El equipo de continuidad analiza el evento ocurrido, y de ser necesario procede a comunicar la situación al comité de crisis.
b. Identificar los procesos críticos afectados, y en caso se proyecte un impacto grave para la organización, convocar al comité de crisis.
c. El líder de comité de crisis convocará al comité de crisis e informará el análisis realizado por el equipo de continuidad.
d. Analizar la necesidad de movilizar las operaciones al centro de comandos alterno.
e. Monitorear constantemente el estado de paralización de las operaciones, verificando que superen el RTO establecido.
f. Mantener la coordinación con los miembros del comité de crisis, indicando la etapa en la que se encuentran: i) Posible desastre: se considera esta etapa cuando al analizar la situación se identifica un evento de crisis generalizado; ii) Alerta de desastre: Cuando analizando la situación se proyecte no recuperar los servicios de forma oportuna; iii) Desastre declarado: Cuando se confirme que los servicios no han sido recuperados dentro de los tiempos establecidos (RTO).
g. Verificar el despliegue de las actividades y planes de recuperación de negocios según el proceso afectado.

5.3 Fase Después – Actividades de restauración y retorno a la normalidad

a. Luego de haber ejecutado las estrategias correspondientes, comunicar que el desastre ha sido controlado.
b. Coordinar el regreso de las operaciones al centro principal.
c. Asegurar que el retorno de las operaciones considere la integridad de la información.
d. Confirmar el retorno a las operaciones.
e. Proceder con la desactivación del centro de operaciones alterno.

6. Gestión de comunicación con medios de prensa, grupos de interés

La gestión de comunicación con los distintos grupos de interés es descrita en el plan de comunicaciones.

7. Criterios de escalabilidad – Árbol de llamadas

En esta sección se establece línea de comunicación que se debe seguir durante la activación y el despliegue del plan de crisis:

Cargo	Rol
Analista Senior de Continuidad del negocio	Equipo Asesor
Gerente de Riesgos	Equipo Asesor
Gerente General	Líder de equipo de crisis
Gerente de Finanzas / Gerente de Negocios / Gerente de Administración	Equipo administrativo

Jefe de Operaciones (líder) Jefe de Finanzas y Tesorería Jefe de Gestión de Personal Jefe de TI Jefe de seguridad Jefe de Logística Oficial de seguridad de la información Gerente de agencia Coordinador de operaciones	Equipo de contingencia

8. Puestos de comando

Para el desarrollo del comité de crisis, se debe contar con un sitio alterno de operaciones en caso se presente inconvenientes en la sede principal.

- Sede de operaciones principal: Oficina administrativa principal ubicada en el distrito de San Borja.
- Sede de operaciones alterna: Instalaciones de la agencia Comas. Se cuenta con un centro alterno, con los equipos listos para operar en las instalaciones de la agencia de Comas.

ANEXO L: Plan de comunicación

1. **Objetivo**:

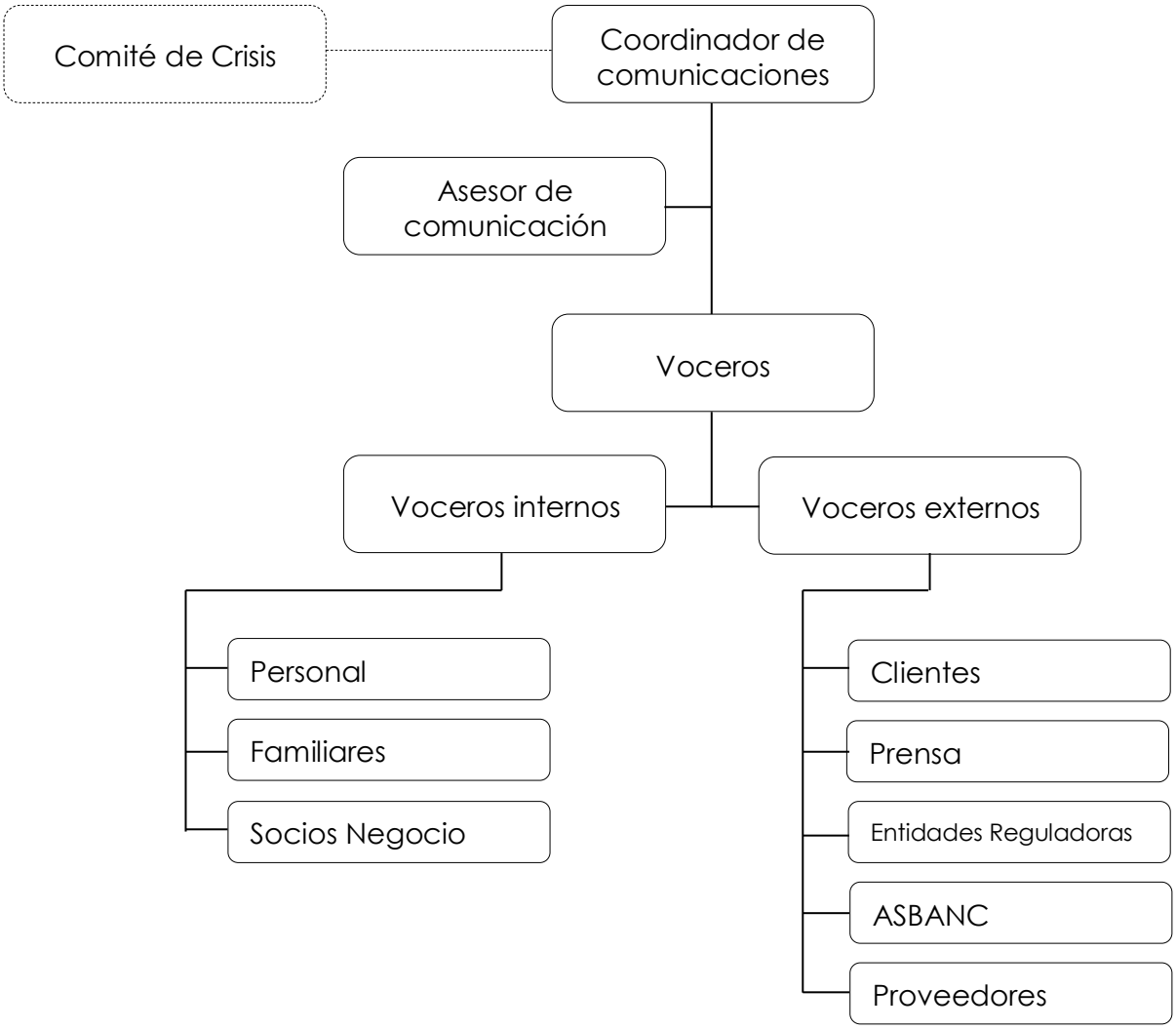
   El plan de comunicación establece un conjunto de actividades cuyo desarrollo permite contar con un sistema de comunicación efectivo ante la presencia de un evento que genere la interrupción de las operaciones de la organización.

2. **Alcance**:

   El plan de comunicación se encuentra orientado a establecer actividades que permitan brindar información sobre el estado en que se encuentra una organización durante y posterior a un evento de crisis. Estas comunicaciones se realizan a diferentes grupos de interés; a nivel interno, al personal, familiares y socios; y a nivel externo, a clientes, no clientes, entidades reguladoras, y proveedores.

3. **Roles y responsabilidades**:

   El plan de comunicación, se encuentra dirigido por el coordinador de comunicaciones (líder del plan de comunicaciones). La estructura de este comité es la siguiente:



- Coordinador de comunicaciones: Esta función es realizada es por la Gerencia General, quien se encuentra a cargo de tomar las decisiones respecto al contenido de las comunicaciones que se emiten a los grupos de interés interesados.

- Asesor de comunicación: Cargo que es desempeñado por el Jefe de Marketing, quien se encuentra encargado de analizar la situación y el impacto que generará informar el estado en que se encuentra la organización a los diferentes grupos de interés.

- Voceros internos: Personal que tiene como responsabilidad brindar a los trabajadores, familiares y socios, información relacionada al estado del evento de crisis.
  El encargado de brindar información, a los trabajadores y familiares es el Jefe de Gestión de Personal, y a los socios el Gerente General.

  Se informará a los trabajadores un comunicado indicando el estado de la organización, asimismo se informará a los familiares del personal cualquier evento de emergencia acontecido y que haya puesto en riesgo la integridad de los trabajadores.

- Voceros externos: Personal que tiene como responsabilidad brindar a la prensa, clientes, entidades reguladoras, ASBANC y proveedores, información relacionada al estado del evento de crisis.
  El encargado de brindar información, a la prensa y a los clientes es el Gerente General (la Gerencia de Negocios asumirá el cargo ante indisponibilidad del titular), para las entidades reguladoras es el Gerente Legal, para el gremio (ASBANC) es el Gerente de Riesgos, y para los proveedores el Jefe de Logística.

  Se informará a la prensa y a los clientes el estado de la organización considerando el criterio de 'mínima información'. Se debe tener en cuenta que se deberá indicar a los clientes que la organización velará por sus intereses.

  Por otra parte, se debe mantener la comunicación con los proveedores de los recursos de comunicación a efectos de contar con la disponibilidad de los mismos.

4. Criterios de invocación

El plan de comunicaciones puede activarse durante cualquiera de los estados de la crisis, en posible desastre, alerta de desastre, y/o desastre declarado.

4.1 Fase antes – Actividades de preparación

- Mantener actualizada las listas de contactos del equipo de comunicación en crisis.
- Mantener disponibles los aspectos logísticos requeridos para la comunicación en crisis (personal, equipos, insumos, registros vitales).
- Tener disponibles las herramientas de comunicación para cada audiencia objetivo.
- Mantener actualizadas las plantillas de comunicación predefinadas.

4.2 Fase durante – Actividades de activación y respuesta

- Esperar la confirmación del comité de crisis, respecto a la activación del plan de comunicaciones; para ello se deben analizar algunas de las siguientes preguntas: ¿Podrían responsabilizar a la organización por el evento ocurrido?, ¿El evento genera

impacto negativo en la imagen de la organización?, ¿Se ha incumplido alguna ley?, ¿el incidente puede ocurrir nuevamente?
- Notificar la activación del plan de comunicaciones a los integrantes correspondientes.
- Verificar la entrega inmediata de los recursos requeridos por el equipo de comunicaciones.
- Discutir, gestionar y aprobar la información, los canales de comunicación, y la estrategia a seguir para desplegar el plan de comunicaciones.
- Realizar la comunicación a las audiencias correspondientes.
- Monitorear y analizar las respuestas y acciones de las audiencias como resultado de las comunicaciones realizadas.

4.3 Fase después – Actividades de desactivación

- Recibir la notificación del comité de crisis para la desactivación del plan de comunicaciones.
- Realizar un informe con el resultado de la ejecución del plan de comunicaciones, identificando el impacto de la crisis en la imagen institucional
- Establecer y proponer estrategias orientadas a mejorar la imagen de la organización.

ANEXO M: **Plan de recuperación de desastres**

1. Objetivo

El objetivo principal de un plan de recuperación de desastres de TI, es reanudar y posteriormente restaurar los servicios que brinda el departamento de TI y que soportan procesos críticos de la organización.

2. Alcance

Los servicios que brinda el departamento de TI, que soportan a procesos críticos de la organización, y que se encuentran contemplados en el plan de recuperación de desastres son:

a) Servicios de Base de Datos: Este servicio considera a las bases de datos de créditos, ahorros, y reclamos.

b) Servicios de conectividad: Se debe verificar el funcionamiento de equipos tales como UPS, firewalls, servidores de dominio, correo, página web, VPN.

c) Aplicaciones: Verificar el correcto funcionamiento de las aplicaciones de créditos y ahorros.

3. Roles y responsabilidades

La organización cuenta con un equipo especializado para la recuperación de los servicios de TI, el cual se encuentra liderado por la Jefatura de Tecnología de Información:

Responsable	Suplente	Responsabilidades
Jefe de Tecnología de Información	Analista Senior de Desarrollo	• Dirigir la reanudación y restauración de los servicios de TI. • Mantener la comunicación con el líder del equipo de continuidad del negocio. • Dirigir la puesta en producción del centro de datos alterno. • Establecer programas de capacitación para el personal del departamento de TI. • Verificar periódicamente la ejecución de copias de respaldo de las versiones de software críticos, de las bases de datos core, y de usuarios clave.
Analista Senior de Producción	Asistente de BD / Asistente de Redes	• Iniciar la recuperación de las aplicaciones de créditos y ahorros.
Administrador de Base de Datos	Analista senior de producción	• Iniciar la recuperación de las bases de datos que soportan a servicios críticos (créditos y ahorros).
Administrador de redes y comunicaciones	Analista senior de producción	• Iniciar la recuperación de los siguientes servicios: servidor de dominio, servidor citrix (para acceso remoto), servidor de

		archivos.

4. Revisión y actualización

El jefe de TI, será el responsable de la revisión del manual de recuperación de desastres, esta actualización se realizará de forma anual, en caso donde se presenten las siguientes situaciones:

- Cambios en el ambiente tecnológico que requieran actualizar los mecanismos contingentes.
- Cambios en niveles de acuerdo de servicios (SLA) con proveedores y servicios de telecomunicaciones.
- Nuevos requerimientos de seguridad exigidos por las entidades reguladoras.
- Cambios significativos en la tecnología utilizada por la organización.
- Mejoras en mecanismos de recuperación.

5. Inventario de activos de tecnología de soporte para los procesos críticos

5.1 Sistemas de información

La organización cuenta con dos aplicaciones core, el sistema de créditos y el sistema de ahorros, cuyo funcionamiento se encuentra a cargo del departamento de tecnología de información.

5.2 Servicio de conectividad

Se debe verificar por la operatividad de la red privada de datos, tecnología que permite la extensión segura de la red para el servicio de conectividad con la red de la empresa. El responsable de velar por el funcionamiento de este servicio es el administrador de redes.

5.3 Servicio de comunicación y mensajería

Se debe verificar por la operatividad del correo electrónico, servicio orientado al envío y recepción de mensajes entre diversos usuarios. El responsable de velar por el funcionamiento de este servicio es el administrador de redes.

5.4 Gestión de accesos y cuentas de usuarios

Con el objetivo de permitir el acceso de los diferentes usuarios a las aplicaciones y otros servicios de TI; uno de los principales servicios que se debe recuperar es el directorio activo, en razón que éste permitirá a los trabajadores clave contar con acceso a la red de la organización, así como a las aplicaciones core.

5.5 Seguridad Perimetral

Si bien se deben recuperar la operatividad de los servicios que brinda la empresa hacia el cliente, se debe tener en cuenta que estos servicios deben contar con un nivel de seguridad adecuado, debido a ello se verificará el correcto funcionamiento

de equipos como firewalls, IPS, IDS, y servidores proxy. El administrador de redes será el responsable de velar por el correcto funcionamiento de estos equipos.

5.6 Servicios web

Se debe contar con acceso y control a los códigos fuente de la página web, así como con acceso a la base de datos SQL en la cual se soporta la aplicación web de reclamos.

5.7 Suministro eléctrico

El departamento de TI en coordinación con el equipo de continuidad y logística serán responsables de velar por que los UPS (Uninterrumptible Power System), y grupos electrógenos se encuentren disponibles para su utilización.

6. Estrategias

6.1 Fase Antes

En esta primera fase se debe verificar que los recursos del departamento de TI se encuentren disponibles para su utilización ante la ejecución del plan de recuperación de desastres, para lo cual se deberá:

- Realizar visitas al CPDA (centro de procesamiento de datos alterno) y validar la existencia y el funcionamiento de los servidores, equipos de operación, utilitarios y registros vitales.
- Realizar pruebas de comunicación con los proveedores y entre el personal participante en este plan.

6.2 Fase Durante

- La jefatura del departamento de TI evaluará la situación, identificando qué servicios no operan correctamente, posteriormente realizará un análisis del impacto que esta interrupción puede ocasionar y en función a ello se comunicará al comité de crisis. De ser necesario se realizarán evaluaciones remotas.
- Realizar las coordinaciones para la conexión de los servicios con la infraestructura que se encuentra en el centro de datos alterno.
- Se realizarán pruebas iniciales tales como, verificación de operación de los equipos, acceso a los sistemas de información.
- Proceder con la ejecución de los planes de reanudación de cada uno de los servicios.

6.3 Fase Después

- El jefe de TI comunicará al equipo de continuidad que el evento ha sido controlado.
- Proceder con las actividades que permitan retornar a los servicios de TI a sus operaciones tal como se encontraban antes del evento disruptivo.
- Realizar pruebas que permitan verificar que los servicios de TI se encuentran operando adecuadamente luego de la etapa de retorno.

- Elaborar informes con el detalle del evento ocurrido, y oportunidades de mejora.